DRAFT Report 16.0

Resarch Paper: Connections to a Trump Organization Server from Alfa Bank (Russia), Spectrum Health (Michigan), and Heartland Payment Systems (New Jersey)

October 4, 2018

Draft Research Report: Not For Public Dissemination

Revisited: Connections to a Trump Organization Server from Alfa Bank (Russia), Spectrum Health (Michigan), and Heartland Payment Systems (New Jersey).

October 4, 2018

Table of Contents

Background

This memo is the result of more than twelve months of research in consultation with experts in cyber security, network administration, and the Domain Name System (DNS). Individuals with significant U.S. intelligence and U.S. law enforcement experience contributed to this review. The data-set of DNS logs referenced throughout this memo (37 million DNS records) is believed to be comprehensive[1] and authentic.

Introduction to Findings

- This memo provides information and analysis on the publicly reported connections to a **Trump Organization** server by **Alfa Bank** (Russia) and **Spectrum Health** (Michigan) in 2016.[2]

- The memo identifies a third party, **Heartland Payment Systems** (New Jersey), that was also consistently connecting to the Trump Organization server from June 21, 2016, to August 22, 2016.[3]

- Other than **Alfa Bank**, **Spectrum Health**, and **Heartland Payment Systems**, no other entities (IP addresses) on the internet sought to consistently connect to the Trump Organization server between May 4, 2016, and September 21, 2016.[4]

- The highly unusual and consistent DNS look-ups[5] of the Trump Organization server suggest that there was a special relationship between the Trump Organization server and servers associated with **Alfa Bank, Spectrum Health**, and **Heartland Payment Systems.** The data does *not* reveal the purpose or intent of the DNS look-ups of the Trump Organization server.

---

[1] The information in this memo is based on a DNS data-set derived from the worldwide collection of DNS queries and responses (referred to collectively in this memo as "DNS look-ups"). The specific DNS data-set reviewed includes more than 37 million DNS queries and responses for a set of domain names and IP addresses from January 1, 2016, to January 15, 2017. The assessments in this memo are based on a belief by researchers that the DNS data-set is comprehensive, representative, and authentic.

[2] https://www.nytimes.com/2016/11/01/us/politics/fbi-russia-election-donald-trump.html?mcubz=1&_r=0; http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html.

[3] On April 25, 2016, Heartland Payment Systems and Global Payments completed a $4.4 billion-valued merger. Years earlier, on December 5, 2011, a company owned by Global Payments, UCS, acquired Alfa Bank's merchant acquiring business for $14.1 million to "significantly expand its presence on the Russian acquiring market." See http://files.shareholder.com/downloads/AMDA-1JAKGZ/5051412914x0x905339/CE3CE356-04AC-4216-8A07-ECA6F8D441F2/GPN_2016_Annual_Report_FINAL.pdf; https://investors.globalpaymentsinc.com/releasedetail.cfm?releaseid=966563; https://ucscards.ru/en/about/history/ NOTE: The Alfa Bank acquisition was reportedly "structured as an asset sale and involved the referral of the existing acquiring clients and transfer of POS-terminals to UCS. The parties also entered into a 10-year cooperation arrangement, with Alfa Bank retaining its role as settlement bank for payments processed by UCS and agreeing to refer clients for merchant acquiring services to UCS." http://www.theasiachronicles.com/recent-deals/dewey-leboeuf-advises-alfa-bank-on-sale-of-merchant-acquiring-business; https://investors.globalpaymentsinc.com/secfiling.cfm?filingid=1123360-13-14&cik=

[4] See chart included in the description of Finding #1.

[5] The use of the term "DNS look-ups" throughout this memo refers to DNS queries and responses.

Memo Structure

This memo begins by providing a summary of public reporting prior to September 2018 on the connections to a Trump Organization server by Alfa Bank and Spectrum Health. The memo then provides detailed information to support the additional research findings below.

Research Findings

1. A review of DNS records indicates that Alfa Bank in Russia, Spectrum Health in Michigan, and Heartland Payment Systems in New Jersey, accounted for nearly all of the DNS look-ups[6] for a specific Trump Organization server, "mail1.trump-email.com," from May 4, 2016, to September 21, 2016.[7]

2. When compared to a similar business on the same network block,[8] the Trump Organization server remains noteworthy for the small number of entities (IP addresses) conducting DNS look-ups of "trump-email.com" and the sustained number of DNS look-ups from Alfa Bank and Spectrum Health.

3. The FBI reportedly concluded in 2016 that there could be an *"innocuous explanation"* for the Alfa Bank *"computer connections"* to the Trump Organization server, such as *"marketing email or spam."* A review of DNS records indicates that the Trump Organization server ("mail1.trump-email.com") was *not* configured to effectively send marketing or bulk email (spam). Moreover, the pattern of DNS look-ups was *not* consistent with automated marketing or bulk email (spam) operations.

4. Testing indicates that the server assigned to the Trump Organization ("mail1.trump-email.com") was configured to accept email.[9]

5. The data indicates that in September 2016 there was likely human interaction and coordination between personnel working on behalf of Alfa Bank (or their designees) and personnel working on behalf of the Trump Organization (or their designees).

6. The Alfa Bank-funded investigations by Stroz Friedberg and Mandiant do not refute the public allegations made regarding the server connections, or the findings of this memo.

---

[6] The use of the term "DNS look-ups" throughout this memo refers to DNS queries and responses.

[7] See attachments for additional information on these three entities.

[8] A network block (or net block) is a range of IP addresses that is owned by a specific internet service provider or data center.

[9] As described in the technical attachment, this finding does not lead our researchers to conclude that the server was exchanging traditional email. In fact, the lack of MX or TXT queries makes it highly unlikely that these four entities were sending ordinary SMTP email amongst themselves. Nonetheless, the DNS data overwhelming points to the fact that there was a special server relationship between the four entities discussed in this memorandum from May 4, 2016, to September 21, 2016. In other words, whatever the purpose of the server named "mail1.trump-email.com," that purpose was something exclusively used by Alfa Bank, Spectrum Health, and Heartland Payments Systems. NOTE: Research into Cendyn software services indicates that Cendyn provides clients with communications and payment sending capabilities via their eProposal and Guestfolio CRM software platforms.

7. The public statements by the Trump Organization, the 2016 Trump campaign, Spectrum Health, and Alfa Bank on the server connections are contradictory and omit pertinent facts. As of September 1, 2018, Heartland Payment Systems has never commented on its server connections to the Trump Organization server.[10]

[10] See chart of public statements attached to this document.

Section One: Overview of Published Media Accounts on the Trump Organization Server[11]

Section One of this memo briefly chronicles the media coverage through September 1, 2018, of the allegations that Alfa Bank and Spectrum Health were uniquely communicating with a Trump Organization server in 2016. This narrative includes reporting on Brian Benczkowski, who leads the Criminal Division of the Department of Justice, and his work in private practice on behalf of Alfa Bank, as well as Benczkowski's public statements that there were no Alfa Bank connections to the Trump Organization.

While the media reporting contains valuable and accurate information, the reporting also includes errors and gaps that subsequent sections of this memorandum address.

On October 31, 2016, just days before the presidential election, *The New York Times* published an article entitled, ***"Investigating Donald Trump, F.B.I. Sees No Clear Link to Russia."*** The *Times* reported that the FBI examined *"computer data showing an odd stream of activity to a Trump Organization server and Alfa Bank,"* but that the FBI *"ultimately concluded that there could be an innocuous explanation, like a marketing email or spam, for the computer contacts."*[12]

On the same day, **Franklin Foer** published an article in *Slate Magazine* entitled, ***"Was a Trump Server Communicating with Russia?"*** *Slate* reported that computer researchers searching for malware identified an *"irregular pattern"* of **Trump Organization** server DNS look-ups by a Russian bank. The look-ups did not appear to be automated, but rather *"resembled the pattern of human conversation."*[13] The researchers concluded that this *"wasn't an attack, but a sustained relationship between a server registered to the Trump Organization and two servers registered to an entity called Alfa Bank."*[14] Other computer experts who reviewed the DNS records vouched for the credibility of the DNS records and noted it would be *"nearly impossible"* to forge or manipulate such data.[15]

According to the Slate piece, the researchers identified several anomalies:

- The **Trump Organization** server was registered in 2009 to conduct consumer marketing campaigns and had a *"history of sending mass emails on behalf of Trump-branded properties and products."*[16] However, the server was later configured to *"accept only incoming communication from a very small handful of IP addresses,"* and handled a

[11] As of September 1, 2018

[12] https://www.nytimes.com/2016/11/01/us/politics/fbi-russia-election-donald-trump.html?mcubz=1. Note: This memo provides a series of facts indicating that the reported FBI assessment is likely inaccurate. For example, the Trump Server was not configured to successfully disseminate marketing or bulk email from May 2016 to November 2016.

[13] http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html

[14] http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html

[15] http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html

[16] http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html

"strangely small load of traffic, such a small load that it would be hard for a company to justify the expense and trouble it would take to maintain it."[17]

- When the researchers *"pinged the server,"* they received error messages suggesting that the **Trump Organization** server was configured to only accept email from specific IP addresses.[18] One of the researchers who examined the data, Indiana University computer scientist **Dr. L. Jean Camp**, told Foer: *"It's pretty clear that it's not an open mail server,"* noting that *"[t]hese organizations are communicating in a way designed to block other people out."*[19]

- In September 2016, shortly after *The New York Times* first contacted **Alfa Bank** about the suspicious DNS look-ups by Alfa Bank, the server associated with the **Trump Organization** *"seemed to suddenly stop working."*[20] The group of researchers reasoned that the Trump Organization *"shut down the server after Alfa was told that the Times might expose the connection."*[21]

- When researchers attempted to look-up the host name, the DNS server *"returned a fail message,"* providing *"evidence that it no longer functioned."*[22] The DNS traffic to the server also *"abruptly"* spiked, as *"servers frantically attempt[ed] to resend rejected messages."*[23]

- The researchers found that less than a week later the **Trump Organization** *"created a new host name," "trump1.contact-client.com,"* which *"enabled communication to the very same server...."*[24] The researchers also found that **Alfa Bank** was the first entity on the internet to look-up the revised host name.[25] Computer experts indicated that it would be impossible for an organization to find the renamed server unless they already knew what the new name was and that the server name had changed.[26]

---

[17]http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html
[18]http://www.slate.com/articles/news_and_politics/politics/2016/11/the_trump_server_evaluating_new_evidence_and_countertheories.html
[19]http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html
[20]http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html
[21]http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html
[22]http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html
[23]http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html
[24]http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html
[25]http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html
[26]http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html

Days later, on November 2, 2016, Foer published a follow-up article in *Slate* providing alternative theories for the server connections, as well as more detailed response statements from the parties involved.[27] Many entities—including the **Trump Organization**—suggested that the DNS traffic might be a result of spam or email marketing.[28] **Cendyn**, a third party vendor that operated the server on behalf of the **Trump Organization**, informed CNN that its contract to provide email marketing services to the **Trump Organization** ended in March 2016, and that a different client had been communicating with **Alfa Bank** using **Cendyn** communications applications.[29] **Alfa Bank** denied this claim.[30]

Listrak—a company in Lititz, Pennsylvania, that maintains servers to send marketing and bulk emails on behalf of corporate clients—was retained by **Cendyn** to host the **Trump Organization** server.[31] In March 2017, Listrak CEO **Ross Kramer** informed a local newspaper that the FBI visited the Listrak office before the 2016 presidential election. Kramer stated the visit was *"very cordial"* and that *"we've given [the FBI] everything they need."*[32] Kramer added: *"If you look back at the election, with all of the allegations swirling around emails ... the domain name 'trump-email.com' is going to get some attention. It's a mystery to me how the (Russian bank) [sic] people got involved with it."*[33]

In March 2017, **Dr. L. Jean Camp** told CNN that it was unusual for just two companies to make up 99 percent of the DNS look-ups of the Trump Organization server, adding: *"If it were spam, then a lot of other organizations would be doing DNS lookups. There would be evidence of widespread connectivity with devices."*[34]

As a result of Camp's public statements, **Alfa Bank**, using the law firm **Kirkland & Ellis LLP**, sent three letters to Dr. Camp and her lawyers, dated March 17, 2017,[35] April 12, 2017,[36] and June 21,

---

[27] http://www.slate.com/articles/news_and_politics/politics/2016/11/the_trump_server_evaluating_new_evidence_and_countertheories.html

[28] http://www.complex.com/life/2016/11/donald-trump-server-communicating-with-russia

[29] http://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/ The article states: "Cendyn is the contractor that once operated marketing software on that Trump email domain. In February, it provided CNN a Trump Organization statement that called the internet records 'incomplete' and stressed that they do not show any signs of 'two-way email communication.' That statement lends credibility to the spam marketing theory, because it says the Trump server was set up in 2010 to deliver promotional marketing emails for Trump Hotels. But Cendyn acknowledged that the last marketing email it delivered for Trump's corporation was sent in March 2016, 'well before the date range in question.'" The article continued: "Cendyn has also provided another possible explanation, suggesting a highly technical case of mistaken identity. Cendyn routinely repurposes computer servers -- like the one used by the Trump Organization. Cendyn's software, like its event planning tool Metron, sends email and thus relies on the 20 different email servers rented by the company. After 'a thorough network analysis,' Cendyn has said that it found a bank client had used Metron to communicate with AlfaBank.com. But Alfa Bank starkly denies 'any dealings with Cendyn.' And, it says, it's unlikely that it received any emails from that server. 'Mandiant investigated 12 months of email archives and it found no emails to or from any of the IP addresses given to us by the media.' On Wednesday, Cendyn provided another explanation to CNN. Cendyn claims the Trump Hotel Collection ditched Cendyn and went with another email marketing company, the German firm Serenata, in March 2016. Cendyn said it 'transferred back to' Trump's company the mail1.trump-email.com domain. Serenata this week told CNN it was indeed hired by Trump Hotels, but it 'never has operated or made use of' the domain in question: mail1.trump-email.com."

[30] http://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/

[31] https://www.listrak.com/about;
http://lancasteronline.com/news/local/fbi-gets-lititz-firm-s-help-in-probe-of-russian/article_ef5d5ed0-05ae-11e7-a003-471e5543b26a.html

[32] http://lancasteronline.com/news/local/fbi-gets-lititz-firm-s-help-in-probe-of-russian/article_ef5d5ed0-05ae-11e7-a003-471e5543b26a.html

[33] http://lancasteronline.com/news/local/fbi-gets-lititz-firm-s-help-in-probe-of-russian/article_ef5d5ed0-05ae-11e7-a003-471e5543b26a.html

[34] http://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/

[35] http://ljean.com/files/AlfaBankThreatLetter.pdf

[36] http://ljean.com/files/AlfaBankLetter2.pdf

2017,[37] all threatening legal action.[38] The partners at **Kirkland & Ellis** representing Alfa Bank were **Viet Dinh** and **Brian Benczkowski**.[39]

Benczkowski has a longstanding relationship with Attorney General **Jeff Sessions**, having previously served as Staff Director for then-Sen. Sessions after Sessions was named Ranking Member of the **Senate Judiciary Committee** in 2009.[40] **Benczkowski** joined Donald Trump's transition team in September 2016, leading the Trump administration's transition team for the Justice Department before returning to private practice following the January 2017 presidential inauguration.[41]

In March 2017, **Benczkowski** began work on behalf of **Alfa Bank** as a private attorney at **Kirkland & Ellis**.[42] On June 5, 2017, President Trump announced his intention to nominate **Benczkowski** to be Assistant Attorney General for the Criminal Division of the Department of Justice.[43]

In July 2017, in advance of his Senate nomination hearing, **Benczkowski** submitted materials to the **Senate Judiciary Committee** on two investigations[44] commissioned by **Alfa Bank**. The first is a November 4, 2016, investigative report marked "*draft*" by **Mandiant**. The second report, overseen directly by **Benczkowski**, was conducted by **Stroz Friedberg** and dated July 19, 2017.

On July 25, 2017, **Benczkowski** testified during his Senate Judiciary Committee nomination hearing that **Stroz Friedberg** had "*conducted this review [of the computer connections] with the view towards taking the results to the FBI and to the Justice Department, which is what my client and my partner did*."[45]

---

[37] http://ljean.com/files/AlfaBankLetter3.pdf

[38] https://www.documentcloud.org/documents/3520990-ABCFAA.html#document/p2

[39] Benczkowski also played a role in Alfa Bank's litigation against the news organization BuzzFeed. According to a press release by the Ranking Member of the Senate Judiciary Committee, Benczkowski also "reviewed the 'Steele dossier,' a private investigator's file on alleged links between Russia and the Trump campaign. He did this for Alfa Bank to consider suing Buzz Feed for defamation over their online publication of the dossier. Alfa Bank, in fact, did sue Buzz Feed on May 26 [2017]." Specifically, Christopher Steele, a former British intelligence officer who was assigned to Russia, provided reporting from sources in the "dossier" that Alfa Bank was involved in an alleged Russian government campaign to influence the results of the November 8, 2016, U.S. presidential election. On August 21, 2018, a federal judge in Washington, D.C. dismissed Alfa Bank's lawsuit against Steele, concluding that his work was covered by the first amendment. https://www.theguardian.com/us-news/2018/aug/21/author-of-trump-russia-dossier-wins-libel-case-in-us-court-christopher-steele

[40] http://www.cnn.com/2017/07/24/politics/brian-benczkowski-alfa-bank/index.html; http://politicalticker.blogs.cnn.com/2009/05/13/sessions-announces-judiciary-staff/; https://www.washingtonpost.com/news/powerpost/wp/2016/11/16/brian-benczkowski-once-dubbed-gops-go-to-guy-for-hearings-helping-manage-justice-department-transition/?utm_term=.80ce743c5faa

[41] https://www.feinstein.senate.gov/public/index.cfm/press-releases?id=71649645-8A75-4C9A-8C45-8CEA26A4D4B7

[42] https://www.feinstein.senate.gov/public/index.cfm/press-releases?id=71649645-8A75-4C9A-8C45-8CEA26A4D4B7 Note: Asked why he accepted Alfa Bank as a client at his Senate nomination hearing, Benczkowski stated: "Well Senator, I'll say this [interruption] Senator, as I was asked to undertake this representation, I was aware that there had been a previous investigation by another law firm and by a very respected computer forensics firm called Mandiant. And it looked at the 2016 allegations and found them to be inaccurate. And there to be nothing to it. And so when the client [Alfa Bank] and Viet [law partner] came to me to represent this, I was comfortable accepting the representation and the work."

[43] https://www.whitehouse.gov/the-press-office/2017/06/05/president-donald-j-trump-announces-intent-nominate-personnel-key

[44] The Mandiant report stated that they conducted their review "in conjunction with Alfa-Bank," that they relied entirely on information provided by Alfa Bank, and that the material necessary to conduct a review of the 2016 server allegations was unavailable. The Stroz Friedberg similarly stated it could not review the 2016 allegations because Alfa Bank did not preserve the required information, stating the data "no longer exists" at Alfa Bank. See http://i2.cdn.turner.com/cnn/2017/images/07/24/dinh.to.grassley.feinstein.pdf

[45] Senate Judiciary Confirmation Hearing for the nomination of Brian Allen Benczkowski, to be an Assistant Attorney General, Criminal Division, Department of Justice, July 25, 2017. https://www.judiciary.senate.gov/imo/media/doc/Benczkowski%20Responses%20to%20QFRs.pdf.

Benczkowski stated in materials submitted to the Senate: "***Mandiant*** *concluded that there was no evidence of* ***substantive*** *[emphasis added] contact, such as emails or financial links, between* ***Alfa Bank*** *and the* ***Trump Organization*** *in 2016*."[46] In his testimony, **Benczkowski** went further, adding that **Mandiant** "*looked at the 2016 allegations and found them to be inaccurate. And there to be nothing to it*."[47]

On July 24, 2017, *The New York Times* suggested that **Alfa Bank**—in the same manner as **Benczkowski**'s testimony—was mischaracterizing the findings of the **Mandiant** report. The *Times* reported:

> *"According to people familiar with Mandiant's review, its experts were shown largely metadata, the information that travels along with a message, for the communications that took place. The contents of the messages — if there were any — were not available.*[48] *Without a much deeper forensic examination, the company could not determine the purpose of the communications. Its resulting report was carefully hedged, noting that without more study, it could not give the bank a clean bill of health. But the bank used that report, however limited, to make the case that it had been exonerated."*[49]

Benczkowski represented to the Senate that "*another independent investigation*," the one that **Benczkowski** directly oversaw by **Stroz Friedberg**, also exonerated **Alfa Bank**.[50] In his confirmation hearing **Benczkowski** testified that "***Stroz Friedberg*** *found that there, once again, was no communication link between the* ***Trump Organization*** *and* ***Alfa Bank.***"[51] The materials submitted by **Benczkowski** to the committee are more specific, and state that the **Stroz Friedberg** investigation "*found no evidence of any connections or communications between* ***Alfa-Bank*** *and the* ***Trump Organization*** *occurring in* ***2017*** *[emphasis added]*."[52] However, as detailed, the only serious allegations of communications between **Alfa Bank** and the **Trump Organization** pertain to 2016, not 2017.

---

[46] http://i2.cdn.turner.com/cnn/2017/images/07/24/dinh.to.grassley.feinstein.pdf

[47] Senate Judiciary Confirmation Hearing for the nomination of Brian Allen Benczkowski, to be an Assistant Attorney General, Criminal Division, Department of Justice, July 25, 2017. https://www.judiciary.senate.gov/imo/media/doc/Benczkowski%20Responses%20to%20QFRs.pdf.

[48] The Mandiant Report claims that the company was provided access to 12 months of the Alfa Bank's email archives, as well as records from the past 6 months for mail server logs, Proxy server logs, and the Deep Discovery Inspector tool. DNS logs were reportedly not retained by Alfa Bank beyond 24-hours. http://i2.cdn.turner.com/cnn/2017/images/07/24/dinh.to.grassley.feinstein.pdf

[49] https://www.nytimes.com/2017/07/24/us/politics/brian-benczkowski-justice-alfa-bank.html?mcubz=1

[50] http://i2.cdn.turner.com/cnn/2017/images/07/24/dinh.to.grassley.feinstein.pdf

[51] Senate Judiciary Confirmation Hearing for the nomination of Brian Allen Benczkowski, to be an Assistant Attorney General, Criminal Division, Department of Justice, July 25, 2017. https://www.judiciary.senate.gov/imo/media/doc/Benczkowski%20Responses%20to%20QFRs.pdf.

[52] http://i2.cdn.turner.com/cnn/2017/images/07/24/dinh.to.grassley.feinstein.pdf

Section Two: What are DNS Records and What Can DNS Records Tell Us?

Worldwide communication on the internet is based on numerical Internet Protocol (IP) addresses that function in a manner similar to telephone numbers. Because large series of numbers are difficult for humans to remember, there is a global **Domain Name System** (DNS) that functions as a phonebook, "*resolving*" (looking-up) easy to remember text-based names (e.g. **www.senate.gov**) into IP addresses (**156.33.241.9**).

DNS look-ups almost always automatically precede and are followed by communication, such as emails, webmail messaging, chat messages, a connection via software, or website visits. There are different types of DNS look-ups. For example, one type of DNS look-up relates to websites;[53] another type of DNS look-up relates to email.[54] Because of this, DNS records can provide insights into the intentions and actions of specific computers.

Before a computer server can send an email, for example, it first must do a DNS look-up to identify the numerical address on the internet of the receiving email server. This is a necessary first step before any two computers can communicate.[55] Below is an example:

- Before a computer can connect with the website "www.banking.senate.gov," the computer must do a DNS look-up of "www.banking.senate.gov" to find the numerical address on the internet of the computer servers handling "www.banking.senate.gov." In the case of "www.banking.senate.gov," the DNS look-up would find the numerical addresses to be "156.33.196,96; 156.33.195.97; 156.33.195.42; 156.33.195.98."

In the internet world of email exchanges and computer connections, **if "Computer X" does a DNS look-up of "Computer Y," it means that "Computer X" is trying to connect to "Computer Y."**[56] An analogy would be a human dialing directory assistance on a telephone and asking for a phone number for a particular business or individual. Acquiring the phone number from the operator is a necessary first step before taking the second step: calling that individual or business. DNS records can reveal attempts to initiate communications and provide insight into intentions, patterns, and types of communications sought.[57]

[53] See https://www.name.com/support/articles/205516858-Understanding-DNS-record-types; https://support.dnsimple.com/articles/a-record/
[54] See https://practical365.com/exchange-server/mx-record/; https://en.wikipedia.org/wiki/MX_record
[55] DNS look-ups alone cannot prove conclusively whether the communication attempt was successful.
[56] DNS look-ups are also conducted by the recipients of communications, in order, for example, to verify the authenticity of emails.
[57] While it is technically accurate to state that DNS logs do not prove that two-way communication took place, it's a misleading statement. While DNS queries do not carry the content of the communication, neither do they happen for no reason. DNS queries almost always happen when a server is attempting to communicate.

Section Three: Summary of Findings

A review of 37 million DNS records identified anomalies and highly unusual connections to a **Trump Organization** computer server from two computer servers assigned to the Russia-based **Alfa Bank**; a server assigned to the Michigan-based health care company, **Spectrum Health**; and, to a lesser extent, a server assigned to the New Jersey-based payment processor, **Heartland Payment Systems**.[58]

As detailed in this memo, additional research found that the **Trump Organization** server was *not* configured to effectively send bulk or marketing email (spam). Further, the DNS look-ups of the server were highly unusual for a marketing server, and its interactions with the internet differed significantly from a similar hospitality entity at an adjacent IP address. The DNS records also indicate that once *The New York Times* alerted **Alfa Bank** that the newspaper was aware of the bank's unusual computer connections to the Trump Organization server, human actions were likely taken by Alfa Bank and the Trump Organization (or their representatives). Finally, investigative reports commissioned by **Alfa Bank** to examine the server connections do not refute the DNS data indicating that an **Alfa Bank** server conducted persistent DNS look-ups of the **Trump Organization** server from May 2016 to September 2016.

[58] These interactions stood out because they were limited to small numbers of computers, repeated over time, and did not match the patterns of automated internet activity.

Section Four: Findings in Detail

Finding #1

1. **A review of DNS records indicates that Alfa Bank in Russia, Spectrum Health in Michigan, and Heartland Payment Systems in New Jersey accounted for nearly all of the DNS look-ups for the Trump Organization server "mail1.trump-email.com" from May 4, 2016, to September 21, 2016.**[59]

As described, the DNS system of communication on the internet is similar to a human dialing directory assistance on a telephone and asking for a phone number for a particular business or individual. The next logical step for the person seeking the phone number for the business or individual is to make the call. In the DNS environment, if "Computer X" makes a DNS look-up for "Computer Y," it means "Computer X" is trying to connect to "Computer Y." DNS look-ups almost always ***automatically*** precede and are followed by communication, such as emails, webmail messaging, chat messages, a connection via software, or website visits. In short, DNS look-ups occur for a reason.

A data-set of more than 37 million DNS records from May 4, 2016 (00:00:00 UTC) to September 21, 2016 (11:33 PM UTC)[60]—which are believed to be comprehensive,[61] authentic, and credible—indicate that there were **3,546** DNS look-ups for the Trump Organization server "**mail1.trump-email.com**."[62]

- Servers associated with **Alfa Bank** and **Spectrum Health** represent **97.67%** of the DNS look-ups of "**mail1.trump-email.com**" during this period.
- **2,761** (77.87%) of the DNS look-ups were from two IP addresses associated with **Alfa Bank**.
- **702** (19.80%) of the DNS look-ups were from an IP address associated with **Spectrum Health**.
- **76** (2.14%) of the DNS look-ups were from an IP address associated with **Heartland Payment Systems**.
- One IP address conducted two (.06%) DNS look-ups of the server, and five other IP addresses each conducted just one DNS look-up of the server. These look-ups all occurred at the same time.[63]

[59] See attachments for additional information on these three entities.
[60] The DNS records reviewed for this memorandum section include data from 00:00:00 UTC May 4, 2016, to 11:33PM UTC September 21, 2016, the date reporters from The New York Times approached Alfa Bank about its connections to "mail1.trump-email.com."
[61] The DNS data-set includes more than 37 million DNS records, or enough worldwide data to provide an accurate overall picture of the IP addresses around the world attempting to communicate with "mail1.trump-email.com."
[62] Using an online DNS estimator tool, 100 inbound emails with a Time-To-Live (TTL) of 5 minutes (as similar to our data) would result in approximately 1.39 DNS queries per email. (https://www.ultratools.com/tools/queryEstimatorTool). This would be approximately 2006 emails related to Alfa Bank, 505 emails related to Spectrum Health, and 55 emails related to Heartland Payment Systems from May 4, 2016, to September 21, 2016. As described in this document, researchers do not believe the servers were exchanging traditional email.
[63] Data-set entitled "DNSLUPSMAIL1082417."

All Entities in Data-Set Attempting to Communicate with the Trump Server *DNS "A" Look-ups* of "mail1.trump-email.com" (66.216.133.29) from 5/4/16 to 9/21/2016 (11:33 PM UTC)*				
Box	**"A" Look-Ups**	**IP Address**	**Entity Association**	**Percentage**
1	1,392	217.12.96.15	Alfa Bank** (Russia)	39.26%
2	1,369	217.12.97.15	Alfa Bank** (Russia)	38.61%
3	702	167.73.110.8	Spectrum Health (MI, USA)	19.80%
4	76	63.241.252.2	Heartland Payment Systems*** (OH, USA)	2.14%
5	2	74.118.76.182	Peer to Peer (Rehoboth, RI, USA)****	0.06%
6	1	98.130.1.253	Ecommerce Corp (OH, USA)***	0.03%
7	1	71.5.34.5	DataCenter.BZ (OH, USA)****	0.03%
8	1	64.98.42.242	Tucows.com (Toronto, CA)****	0.03%
9	1	54.206.26.93	Amazon Web Services (AUS)****	0.03%
10	1	205.134.252.154	InMotion Hosting (Los Angeles, CA, USA)****	0.03%
Total	**3,546**			**100%**

* This table summarizes DNS "A" address queries[64] for "**mail1.trump-email.com**." Researchers also reviewed DNS "PTR" reverse name queries for 66.216.133.29 (the IP address associated with "**mail1.trump-email.com**"). Researchers found DNS "PTR" reverse name queries that originated from 167.73.110.8 (the IP address associated with Spectrum Health). This indicates, with a high degree of certainty, that persistent and sustained connections existed between the referenced Spectrum Health server and the "**mail1.trump-email.com**" server, and that these were not random or accidental DNS query packets.

** Alfa Bank combined DNS look-ups for "**mail1.trump-email.com**" equals **2,761**, or **77.87%**.

*** DNS look-ups began on June 21, 2016, and ceased on August 22, 2016.[65]

**** The DNS look-up/s for these entities all occurred at similar times.

[64] An "A" address query is used for the conversion of domain names to corresponding IP addresses (numbers). For example, mail1.trump-email.com converts to 66.216.133.29. "PTR" reverse name queries are used to look up domain names based on an IP address. For example, 66.216.133.29 to mail1.trump-email.com.

[65] Data-set entitled "DNSLUPSMAIL1082417."

Finding #2

> **2. When compared to a similar business on the same network block,[66] the Trump Organization server remains noteworthy for the small number of entities (IP addresses) conducting DNS look-ups of "trump-email.com" and the sustained number of DNS look-ups from Alfa Bank and Spectrum Health.**

Research and analysis were conducted to assess whether the DNS look-ups related to the **Trump Organization's** "trump-email.com" were consistent with a similar, but smaller, hospitality organization also using Cendyn's products and services.

From **Cendyn**'s marketing materials,[67] researchers identified **Denihan Hospitality Group** (DHG) as a Cendyn customer. **Cendyn** registered the domain name "denihan-email.com" on behalf of **DHG** on August 15, 2009[68] (*Note*: **Cendyn** registered the domain name "trump-email.com" on behalf of the **Trump Organization** the day before, on August 14, 2009).[69] The **DHG** servers analyzed by researchers are located on the same network block as the **Trump Organization** server, "mail1.trump-email.com" [66.216.133.29], and are located at adjacent IP addresses [66.216.133.30, 66.216.133.31]. On February 3, 2014, **Listrak** updated the registration for the IP range 66.216.133.0 – 66.216.133.255. This range included the respective servers associated with **DHG** [66.216.133.30, 66.216.133.31] and the **Trump Organization** [66.216.133.29].

According to **DHG** materials, **DHG** identifies as a *"privately-held, full service hotel management and development company."*[70] The company *"owns and/or operates boutique hotels in major urban markets throughout the U.S.,"* including *"properties operating under The James and Affinia Hotel Collection brands, as well as Manhattan independent boutique hotels, The Benjamin, and The Surrey."*[71]

---

[66] A network block (or net block) is a range of IP addresses that is owned by a specific internet service provider or data center.

[67] https://www.prweb.com/releases/cendyn/denihan/prweb2575944.htm

[68] https://www.godaddy.com/whois/results.aspx?domain=denihan-email.com&recaptchaResponse=03AL4dnxovJuQ8oWQylzY7Qd0OF2ELVh6W9paAP9Qe4kOU5vpShtlvsNAovBflqbpq1TGrs_MUhfNVBFrOkfuN0LSn7np-JrkCgjlZYw68Bh9hjJLWaXeF0qhZ-iEyFAVy-T3QKZSzER_b49ZR5RSHVcF1KjMtEco9yNKjLy-zzKR6RNEmNqB6h1MMAmpTs8rM_XNF16vlblBDNLKOgx08aEc74P4RpVWyxnqZv8Dc1gBMoERJTAk2ZDgvFxbujzK4JRr8IDTfD3PpZxBVNCqw-eDKf5ps6LHFDw

[69] http://www.ljean.com/NetworkRecords/Trump-Owned-And-Mail-Systems-WHOIS-15.txt

[70] https://www.apnews.com/4e6a7c622266406592e6d3fd9f0e8a8d; https://www.businesswire.com/news/home/20180521005254/en/Denihan-Hospitality-Appoints-Michael-Goldrich-Vice-President

[71] https://www.apnews.com/4e6a7c622266406592e6d3fd9f0e8a8d; https://www.businesswire.com/news/home/20180521005254/en/Denihan-Hospitality-Appoints-Michael-Goldrich-Vice-President

In July 2016, **DHG** owned and/or operated 10 boutique hotels with 2,704 rooms.[72] In 2014, **DHG** had approximately 2,500 employees.[73] **DHG** reported $280.8 million in annual revenue in 2012.[74]

By comparison, the **Trump Organization** is a privately held conglomerate of approximately 500 different companies[75]—including **Trump Hotels** (formerly the **Trump Hotel Collection**)[76]—that owns, markets, operates, or manages dozens of hotels, residences, and golf courses around the world.[77]

In July 2016, **Trump Hotels** owned and/or operated 9 domestic and international hotel properties with 4,132 rooms.[78] According to a 2016 CNN article, the **Trump Organization** reported $9.5 billion in revenues in 2015.[79] A December 2016 article in *The New York Times* stated that industry experts believe *"no more than 4,000 people work for the **Trump Organization** worldwide."*[80]

[72] To calculate the total number of rooms owned and/or operated by Trump Hotels and DHG, researchers used The Wayback Machine by Internet Archive for the dates of July 1, 2016, through July 31, 2016. Researchers reviewed digital archives of company-hosted websites for hotels that were owned and/or operated by DHG and Trump Hotels. Researchers reviewed digital archives of third-party marketing materials where primary sources were unavailable. *See* the Appendix for details on these calculations.

[73] https://www.linkedin.com/company/denihan-hospitality-group/

[74] https://skift.com/2013/08/21/the-fastest-growing-travel-companies-in-america-in-2013/

[75] https://assets.donaldjtrump.com/Tax_Doc.pdf

[76] https://www.trump.com/trump-hotels/
https://www.trump.com/trump-hotels/

[77] https://money.cnn.com/2016/12/29/news/donald-trump-golf-courses/index.html; https://therealdeal.com/issues_articles/the-8-billion-dollar-man/

[78] To calculate the total number of rooms owned and/or operated by Trump Hotels and DHG, researchers used The Wayback Machine by Internet Archive for the dates of July 1, 2016, through July 31, 2016. Researchers reviewed digital archives of company-hosted websites for hotels that were owned and/or operated by DHG and Trump Hotels. Researchers reviewed digital archives of third-party marketing materials where primary sources were unavailable. *See* the Appendix for details on these calculations.
https://web.archive.org/web/20160727134934/http://www.trump.com:80/hotel-collection;
https://web.archive.org/web/20160723083319/http://www.trump.com:80/hotel-collection/florida/trump-national-miami/;
https://web.archive.org/web/20160801122722/http://www.trump.com:80/hotel-collection/hawaii/trump-intl-hotel-waikiki-beach/;
https://web.archive.org/web/20160731132031/http://www.trump.com:80/hotel-collection/chicago/trump-intl-hotel/;
https://web.archive.org/web/20160728021723/http://www.trump.com:80/hotel-collection/las-vegas/trump-intl-hotel/;https://web.archive.org/web/20160727135112/http://www.trump.com:80/hotel-collection/new-york/trump-intl-hotel;
https://web.archive.org/web/20160803070735/http://www.trump.com:80/hotel-collection/soho/trump-soho;
https://web.archive.org/web/20160801122827/http://www.trump.com:80/hotel-collection/panama/trump-ocean-club;
https://web.archive.org/web/20160727115259/http://www.trump.com:80/hotel-collection/toronto/trump-intl-hotel/;
https://web.archive.org/web/20160727124157/http://www.trump.com:80/hotel-collection/ireland/trump-hotel-golf-links

[79] http://money.cnn.com/2016/12/15/investing/trump-organization-48th-largest-private-company/index.html

[80] https://www.nytimes.com/2016/12/25/us/politics/trump-organization-business.html?_r=0

Denihan Hospitality Group (DHG) - July 2016	Trump Hotels - July 2016
Denihan Hospitality Group (DHG) identifies as a privately held full-service hotel management and development company.[81] In July 2016, DHG owned and/or operated 10 hotel properties in the United States with 2,704 rooms.[82] The hotel properties include: 1. Garden Suites Hotel by Affinia (FKA Lyden Gardens and Affinia Gardens) (New York), 2. Shelburne Hotel & Suites by Affinia (FKA Shelburne Murray Hill) (New York), 3. Fifty Hotel & Suites by Affinia (FKA Affinia 50) (New York), 4. Dumont NYC (FKA Affinia Dumont) (New York) (sold October 2016),[83] 5. The Benjamin (New York), 6. Manhattan NYC (FKA Affinia Manhattan and Southgate Tower Hotel) (New York) (sold October 2016),[84] 7. The James Hotel Chicago – Magnificent Mile, 8. The Surrey (New York), 9. The James New York – Soho, 10. The James New York – NoMad (FKA The Carlton).[85]	According to the company's website, the Trump Organization is a privately owned international conglomerate that includes Trump Hotels, Trump Winery, Trump Golf, Trump International Realty, and the organization's corporate division.[86] In July 2016, Trump Hotels owned and/or operated 9 hotel properties in the United States, Canada, Panama, and Europe with 4,132 rooms.[87] The hotel properties include: 1. Trump® National Doral Miami, 2. Trump® International Hotel Waikiki (Hawaii), 3. Trump International Hotel & Tower® Chicago, 4. Trump® International Hotel Las Vegas, 5. Trump International Hotel & Tower® in New York, 6. Trump SoHo [Hotel] (New York), 7. Trump International Hotel & Tower Panama, 8. Trump International Hotel & Tower Toronto, 9. Trump International Golf Links® & Hotel in Doonbeg (Ireland).

[81] https://www.apnews.com/4e6a7c622266406592e6d3fd9f0e8a8d

[82] https://web.archive.org/web/20160711022924/http://www.denihan.com:80/portfolio/hotel-brands
To calculate the total number of rooms owned and/or operated by Trump Hotels and DHG, researchers used The Wayback Machine by Internet Archive for the dates of July 1, 2016, through July 31, 2016. Researchers reviewed digital archives of company-hosted websites for hotels that were owned and/or operated by DHG and Trump Hotels. Researchers reviewed digital archives of third-party marketing materials where primary sources were unavailable. *See* the Appendix for details on these calculations.

[83] https://therealdeal.com/2016/10/20/pebblebrook-denihan-split-portfolio-of-6-manhattan-hotels/

[84] https://therealdeal.com/2016/10/20/pebblebrook-denihan-split-portfolio-of-6-manhattan-hotels/

[85] https://web.archive.org/web/20160711022924/http://www.denihan.com:80/portfolio/hotel-brands;

[86] http://www.trump.com/the-trump-organization/ Note: The Trump Organization also manages various commercial and residential properties and has licensed its name to multiple national and international residential and commercial projects (some of which have not been built) in India, China, Georgia, Azerbaijan, India, the Dominican Republic, Indonesia, Dubai, Toronto, Turkey, the Philippines, and Uruguay (https://www.trump.com/real-estate-portfolio/).

[87] To calculate the total number of rooms owned and/or operated by Trump Hotels and DHG, researchers used The Wayback Machine by Internet Archive for the dates of July 1, 2016, through July 31, 2016. Researchers reviewed digital archives of company-hosted websites for hotels that were owned and/or operated by DHG and Trump Hotels. Researchers reviewed digital archives of third-party marketing materials where primary sources were unavailable. *See* the Appendix for details on these calculations.
https://web.archive.org/web/20160727134934/http://www.trump.com:80/hotel-collection;

Using the same sources and methods used to obtain the DNS data for "**trump-email.com**," researchers obtained DNS data for "**denihan-email.com**."[88] The **DHG** sample contains 20,605 DNS look-ups spanning a 48-day period from August 4, 2016, to September 22, 2016. These dates overlap with the DNS data available for the **Trump Organization** server, and allows for a comparison between the two organizations in terms of the volume of DNS look-ups and the number of entities (IP addresses) conducting DNS look-ups during the August 4, 2016, to September 22, 2016, period.[89]

Comparison of the Two Organizations & Summary of the DNS Look-Ups for "trump-email.com" and "denihan-email.com." August 4, 2016 – September 21, 2016			
		Comparison	
Box		DHG	Trump Organization
A	Number of Hotels Owned and/or Operated by Each Company in July 2016	10	9
B	Number of Rooms in Hotels Owned and/or Operated by Each Company in July 2016	2704	4132
C	Approximate # of Employees	2500	4000
D	Timestamp of First DNS Look-up	2016-08-04 T00:00:13	2016-08-04 T00:06:35
E	Timestamp of Last DNS Look-Up	2016-09-21 T23:57:02	2016-09-21 T23:33:35
F	Time Period Covered	48 Days	48 Days
G	Total DNS Queries	**20,507**	**2,537**
H	Number of Unique Entities (IPs) Conducting DNS Look-Ups	**1052 IPs**	**10 IPs***
I	Number of Unique Entities (IPs) Conducting More than Two DNS Look-Ups	**769 IPs**	**4 IPs***
J	Sustained Connections with an Organization Over the 48-Day Time Period	0	2**
K	Number of Look-Ups from Alfa Bank Servers for Time Period	0	2051

https://web.archive.org/web/20160723083319/http://www.trump.com:80/hotel-collection/florida/trump-national-miami/;
https://web.archive.org/web/20160801122722/http://www.trump.com:80/hotel-collection/hawaii/trump-intl-hotel-waikiki-beach/;
https://web.archive.org/web/20160731132031/http://www.trump.com:80/hotel-collection/chicago/trump-intl-hotel/;
https://web.archive.org/web/20160728021723/http://www.trump.com:80/hotel-collection/las-vegas/trump-intl-hotel/;https://web.archive.org/web/20160727135112/http://www.trump.com:80/hotel-collection/new-york/trump-intl-hotel;
https://web.archive.org/web/20160803070735/http://www.trump.com:80/hotel-collection/soho/trump-soho;
https://web.archive.org/web/20160801122827/http://www.trump.com:80/hotel-collection/panama/trump-ocean-club;
https://web.archive.org/web/20160727115259/http://www.trump.com:80/hotel-collection/toronto/trump-intl-hotel/;
https://web.archive.org/web/20160727124157/http://www.trump.com:80/hotel-collection/ireland/trump-hotel-golf-links

[88] A CSV file in the same format as previous samples, consisted of timestamp, source IP, QNAME, and query result.

[89] When studying trump-email.com, we cut off our sample at 23:59:59 on 2016-09-21, because on September 22, 2016, publicity around trump-email.com drew traffic that was likely a mix of researchers, curiosity-seekers, and potential hackers. The remainder of this analysis is based on the set of queries for both servers that are between the timestamps 2016-08-04T00:00:00 and 2016-09-21T23:59:59.

Comparison of the Two Organizations & Summary of the DNS Look-Ups for "trump-email.com" and "denihan-email.com." August 4, 2016 – September 21, 2016			
		Comparison	
Box		DHG	Trump Organization
L	Number of Look-Ups from Spectrum Health Servers for Time Period	0	464
M	Number of Look-Ups from Heartland Payment Systems Server for Time Period	0	15
*Two the Four IPs are associated with Alfa Bank. ** Alfa Bank and Spectrum Health			

DHG owned and/or operated fewer hotel rooms (2,704) than the Trump **Organization** owned and/or operated (4,132), yet **DHG** received a substantially higher number of DNS look-ups from a far more diverse number of unique entities (IP addresses). Specifically, while **DHG** is two-thirds the size of the **Trump Organization** in terms of hotel rooms owned/operated, the **DHG** servers received almost 10 times as many DNS look-ups as the **Trump Organization** (20,507 versus 2,537) during the same 48-day period. Moreover, the 20,507 DNS look-ups of **DHG** servers were widely distributed among 1,052 unique entities (IP addresses).[90]

By contrast, the 2,537 DNS look-ups of the **Trump Organization** server came from just 10 unique entities (IP addresses). If the data is limited to entities (IP addresses) conducting more than two DNS look-ups during this 48-day period, the contrast becomes even more stark: **DHG** was communicating with 769 unique entities (IP addresses) over the 48-day period, while the **Trump Organization** was communicating with just four: two associated with **Alfa Bank** (217.12.96.15 and 217.12.97.15), one associated with **Spectrum Health** (167.73.110.8) and one associated with **Heartland Payment Systems** (63.241.252.2).

While the two companies—the **Trump Organization** and **DHG**—have similar businesses, the servers associated with **Alfa Bank, Spectrum Health**, and **Heartland Payment Systems** are not found in the **DHG** DNS data.

In addition to the *volume* of DNS look-ups and the number of unique entities (IP addresses) conducting the DNS look-ups, the pattern over time of the DNS look-ups is significantly different for the two organizations. Most of the entities (IP addresses) conducting DNS look-ups of the DHG server appear sparsely over the 48-day period and the DNS look-ups are correlated to specific times.[91] For example, during the 48-day period of interest, there are times when there

[90] Except for an IP address associated with Amazon Web Services (54.206.26.93), the five random "junk" entities conducting DNS look-ups of the Trump Organization server also conducted DNS look-ups of the DHG servers.

[91] The Denihan DNS sample contains queries from over a thousand IP addresses and 400 distinct networks. The majority of observed DNS look-ups appear in two patterns. The vast majority of the DNS look-ups are what we call Type A clients. These are clients conducting DNS queries of Denihan sparsely, with days or weeks between events. The DNS queries from Type A clients are often correlated in time, creating widely dispersed "type A bursts." A far smaller number of entities are what we call Type B clients. Type B clients conduct occasional intense DNS look-

are bursts of DNS look-ups of the **DHG** server from a broad range of entities (IP addresses). The entities (IP addresses) looking up the **DHG** server are then either completely dormant, or there are significant gaps in time before they communicate with the **DHG** server again. Researchers indicate that this behavior may be in response to some action first taken by the **DHG** server itself, for example, a marketing email being sent from one of its servers. In contrast, the top three entities (IP addresses) conducting DNS look-ups of the **Trump Organization** server all exhibit constant, sustained interaction over the 48-day period.[92] In addition, these DNS look-ups of the **Trump Organization** server, while consistent, do *not* appear to match activity reflecting an automated process (such as in the case of the suspected mass marketing email referenced above in the context of the **DHG** sample).

ups, lasting up to a few days, before ceasing. Notably, the Type B interactions usually begin at the same time as the "Type A" bursts. A smaller number of entities, which represent 5 of the top 6 entities ranked by total volume of DNS look-ups, conduct a large number of sustained DNS inquiries, but remain inactive at times. Since we know Cendyn's business is email marketing, it is possible that Type A DNS queries come from servers that were triggered in some way by a broad-spectrum action initiated at Cendyn, such as sending a bulk marketing email. If these vertically-correlated Type A bursts represent the start of a marketing campaign, then it may be that the Type B DNS queries (which initially resemble Type A Clients) are follow-up contacts to a bulk marketing email. In contrast to Denihan, the queries for the Trump Organization server coming from Alfa Bank and Spectrum Health are sustained during the entire 48-day period. Heartland Payment Systems is active sporadically for a distinct period of time. The remaining 6 entities all appeared to conduct a DNS look-up of the Trump Server at similar times, not unlike the Type A query detailed above.

[92] The three entities (IP addresses) are associated with Alfa Bank (two IPs) and Spectrum Health (1 IP).

Finding #3

3. **The FBI reportedly concluded in 2016 that there could be an "*innocuous explanation*" for the Alfa Bank *"computer connections"* to the Trump Organization server, such as *"marketing email or spam."* A review of DNS records indicates that the Trump Organization server ("mail1.trump-email.com") was *not* configured to effectively send marketing or bulk email (spam). Moreover, the pattern of DNS look-ups was *not* consistent with automated marketing or bulk email (spam) operations.**

Note: On October 31, 2016, *The New York Times* reported that FBI "*officials spent weeks examining computer data showing an odd stream of activity to a Trump Organization server and Alfa Bank,*" but that the FBI "*ultimately concluded that there could be an innocuous explanation, like a marketing email or spam, for the computer contacts*."[93] Analysis of DNS records indicate the reported FBI conclusion was inaccurate.

(a) ***"Mail1.trump-email.com" Was Not Included in the SPF Record:*** In 2016, a computer server named "**mail1.trump-email.com**" was operating on the Trump Organization computer server network. The server name was first established on August 14, 2009.[94] The name of this Trump Organization computer server, "**mail1.trump-email.com**" (referred to as an "A" name) was similar to other Trump Organization server names. The numerical IP address (66.216.133.29) of "**mail1.trump-email.com**" was among a block of other servers contracted for commercial communication purposes (such as bulk marketing email and Customer Relations Management[95] software for hospitality companies),[96] but "**mail1.trump-email.com**" was ***not*** configured like other Trump Organization email servers,[97] nor did it behave like a commercial bulk email server, or like the other commercial servers on the same network block[98] (*See* Finding #2).[99]

---

[93] https://www.nytimes.com/2016/11/01/us/politics/fbi-russia-election-donald-trump.html?mcubz=1

[94] See WhoIs records at http://www.ljean.com/NetworkRecords/Trump-Owned-And-Mail-Systems-WHOIS-15.txt

[95] Note: In the corporate world, Customer Relationship Management (CRM) software, or other special purpose portals, may be set-up on servers for communication exclusively with preferred partners or prospects. For example, the same server where a hospitality company logs-in to manage meetings may have multiple messaging and meeting services, including email capabilities. Research on Cendyn software capabilities revealed that its software suite offers communications and payment sending capabilities via their eProposal and Guestfolio CRM software.

[96] Listrak is a Lititz, Pennsylvania, company that maintains servers to send marketing and bulk emails on behalf of corporate clients, including the Trump Organization. For more information, see http://lancasteronline.com/news/local/fbi-gets-lititz-firm-s-help-in-probe-of-russian/article_ef5d5ed0-05ae-11e7-a003-471e5543b26a.html

[97] As noted elsewhere, the network configuration of "mail1.trump-email.com" shows that it was set-up to use at least Port 25, the port used for email, and was configured with SMTP software. Also, according to a third-party analysis, the volume and cadence of the DNS traffic is indicative of human-controlled communications like email. However, other evidence indicates that this server was not likely being used for standard SMTP email. As described in this section, the server was not included in the SPF record for the Trump Organization domain and no MX queries were observed in the data, which rules out standard email, including for bulk marketing. See appendix for additional information.

[98] A network block (or net block) is a range of IP addresses that is owned by a specific internet service provider or data center.

[99] Note: According to advertising claims by Listrak (which operated the Trump Organization Server on behalf of Cendyn) and its software vendor Port25, Listrak's bulk email servers are capable of sending an average of 2.5 million emails per hour, many orders of magnitude higher than what was observed from this Trump server (See https://port25.com/wpcontent/uploads/downloads/2015/01/Listrak-Case-Study.pdf; "Marketing automation vendor Listrak deploys on average 2.5 million emails per hour per server." It is also notes that "The company's top 20 marketers average roughly 800K subscribers each.") An examination of DNS records for a server right next to the Trump server in this address block, operated on behalf of Denihan Hospitality Group, during this same timeframe, shows significantly less volume of traffic than the advertised bulk email capabilities of Listrak, but still 100 times the number of connections in terms of volume and diversity as compared to the Trump server. The Trump server interacted consistently with only three companies, making a handful of connections daily (Daily volumes ranged from single digits

What is a SPF Record?

Sender Policy Framework ("SPF") is an email authentication protocol on the internet under which the owner of an email domain (such as gmail.com, or trump-email.com) publishes a list of IP addresses in the Domain Name System (DNS) that are authorized to send outgoing email from that domain. This allows spam filters to easily check if the origin of an email is actually from an authorized domain. Some email providers, including some large Fortune 500 companies, are configured to refuse incoming email if the SPF authorization check fails.[100] As such, if you are in the business of sending marketing or bulk email, you would want your servers to be included in an appropriate SPF record to ensure that your emails are successfully delivered to the largest number of users.[101]

A check of public online DNS databases shows the **Trump Organization** controlled the domain name "**trump-email.com**," which includes "**mail1.trump-email.com**."[102] While the domain "trump-email.com" had an SPF authorization record, that SPF authorization record did not include the "**mail1.trump-email.com**" server.[103] This means that "**mail1.trump-email.com**" was configured in such a way that would have prevented it from effectively sending marketing or bulk emails.[104]

---

to double digits, until the trump-email.com zone was deleted on September 23, 2016, at which time volumes spiked to thousands a day caused by Spectrum Health trying to reconnect to the missing hostname, mail1.trump-email.com). Trump vendor Cendyn has stated that their contract to send marketing emails for Trump ended in March 2016.[99] The stated change away from bulk marketing email is congruent with the change seen in the DNS data— from May 2016 through September 2016 the Trump server was only making a small, focused number of connections with three other entities.

[100] A failed SPF look-up, even the "softfail" form embedded in the DNS record for the Trump server ("~all") is detrimental for email delivery. Thus, it is unlikely that "mail1.trump-email.com" was used for sending messages, including marketing messages, on behalf of the parent zone, "trump-email.com."

[101] https://blog.returnpath.com/how-to-explain-spf-in-plain-english/; https://postmarkapp.com/blog/explaining-spf; http://www.openspf.org/Introduction;

[102] See https://www.godaddy.com/whois/results.aspx?domain=trump-email.com&recaptchaResponse=03AOmkcwKPCwjGn0ORdD80csoynKgB-Tp-8bZSaBqt_7uSTF32t6gz4hvKSaBMlimx27aTDuGsjVjpAEge9APOG5-6C5ElyZDlTTwm42khMWQ2v60kdDkckWSK5bXm0nHKLlyYWLkbJ5bmMxkKWlUyU0QhsEdFZBBq47S6iBNlF44a7U-XJnwFycY9rY72U1Chiow2xcK5ihr2VYqA0IeupLSFtvjSOr-mlpHFlIr_AsagUYDMsU3IgaZ_Yer2Y4wbMXS5saXztJ0wXFbbnpQQisR5hCRnnC-u8kIPFRrgnk3JgJ0nDhK9C9-X2wW_eJmHBpp3ckz2wlhwBNLpjrywApqrPMHhxWrXnWl9p9JlXvGQnttLbNxAlmFNzlAnwB0iWTsmj7VzC2dG

[103] See additional data available which details how public online passive DNS databases, such as the DNS informational site dnsdb.io, show several Resource Record sets [RRsets] in the trump-email.com zone. In relevant part these include: ("mail1.trump-email.com A 66.216.133.29." "trump-email.com TXT |v=spf1 ip4:198.91.42.0/23 ip4:64.135.26.0/24 ip4:64.95.241.0/24 ip4:206.191.130.0/24 ip4:63.251.151.0/24 ip4:69.25.15.0/24 mx ~all"). The last line is a Sender Policy Framework ("SPF") record, and identifies domains and address ranges used in outbound email. While complex, the SPF record essentially lists the machines authorized to send outbound email on behalf of the trump-email.com domain. The listed IP address ranges include mail servers that send emails, such as office correspondence. SPF can help recipients identify fraudulent messages (e.g., spam from 3rd party networks claiming to come from trump-email.com). If the sending host claims to come from trump-email.com, but is not inside one of the listed SPF ranges, mail recipients are alerted that the mail may be fraudulent under Internet Engineering Task Force protocol and are therefore more likely to reject the email or to label it as spam. Importantly, the SPF CIDR ranges in this case did not encompass 66.216.133.29, the address for "mail1.trump-email.com." Thus, the SPF record for the Trump Organization server conveyed a policy of advising mail recipients to discard mail from this server. As such, no competent email marketing service provider would intentionally set up an email operation in this way. A mistake in setting a mail server up in this manner would have been rapidly detected and corrected. For email marketing operations, delivery to inboxes rather than spam folders is of paramount importance. A failed SPF lookup, even the "softfail" form embedded in the DNS record for the Trump Organization server ("~all") is detrimental for email delivery. Thus, it is unlikely that "mail1.trump-email.com" was used for sending messages, including marketing messages, on behalf of the parent zone, "trump-email.com."

[104] Additional Evidence that the Trump Organization Server was not Sending Traditional Email: If "mail1.trump-email.com" was being used for mail marketing purposes, recipient organizations would have made DNS queries to retrieve the SPF record to authenticate the email. However, the DNS records show no queries for the SPF text record – no type 16 text queries at all. Moreover, third-party tests conducted during the period

SPF Authorization Record for trump-email.com[105]
trump-email.com TXT |v=spf1 ip4:**198.91.42.0/23** ip4:**64.135.26.0/24** ip4:**64.95.241.0/24** ip4:**206.191.130.0/24** ip4:**63.251.151.0/24** ip4:**69.25.15.0/24** mx ~all[106]
NOT INCLUDED IN SPF RECORD: **mail1.trump-email.com A 66.216.133.29**

(b) ***"Mail1.trump-email.com" Was Not Identified as a Sender of Spam:*** If "**mail1.trump-email.com**" had been used to send marketing or bulk emails, researchers would expect to find the IP address for "**mail1.trump-email.com**" in public spam block lists.[107] In other words, if large amounts of marketing emails were emanating from "**mail1.trump-email.com**," it's likely that some receivers of those emails would have marked them as spam.[108] However, in a search of 57 public spam block lists, the only list that contains the IP address (**66.216.133.29**) for "**mail1.trump-email.com**," is dnsbl.spfbl.net, which appears to enforce SPF configuration based on its self-description (as described, while the domain "trump-email.com" had an SPF authorization record, that SPF authorization record did **not** include the "**mail1.trump-email.com**" server).[109]

in question show that Alfa Bank consistently performed SPF/DKIM authentication look-ups as a matter of practice. This provides additional evidence that the Trump Organization server was not sending marketing email.

[105] https://dnsdb.io/en/search?q= trump-email.com, identified in 2016. Public online passive DNS databases, such as the DNS informational site dnsdb.io show records related to the trump-email.com zone.

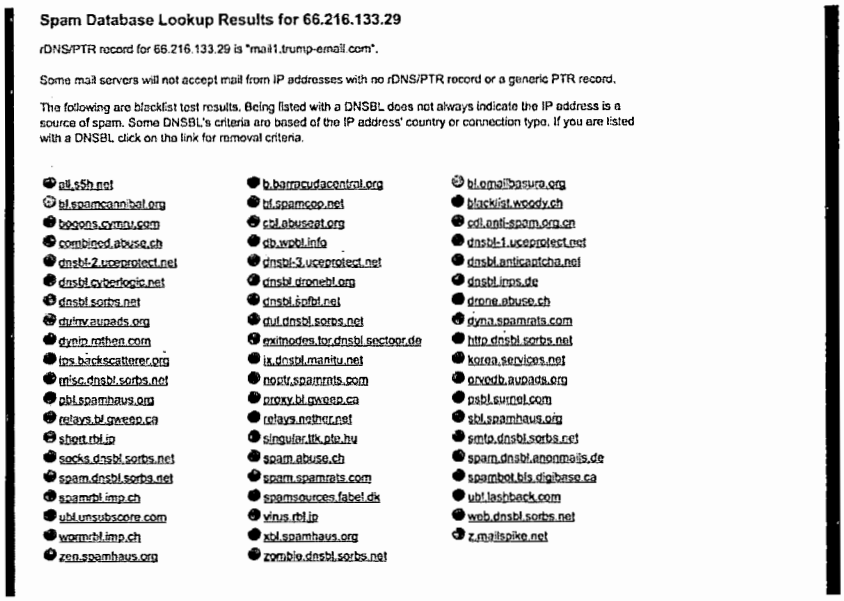
[106] "~" indicates a "softfail" recommendation.

[107] See http://www.slate.com/articles/news_and_politics/politics/2016/11/the_trump_server_evaluating_new_evidence_and_countertheories.html; which includes the following from Dr. L. Jean Camp, a computer expert, who says, "It's highly implausible that spam would continue for so many months, that it would never be reported to a spam blocker, or that nobody else in the world would see the spam during that time frame."

[108] The search for the IP address (66.216.133.29) associated with the Trump Organization Server was conducted in September 2017. It is unclear, as of September 17, 2017, how long IP addresses associated with spam remain on the public spam block lists. Previous researchers have indicated that similar searches conducted during the May 2016 to September 2016 time period also failed to identify the IP address as a sender of spam.

[109] See http://spfbl.net/en/dnsbl/

57 Public Spam Block Lists[110]



Spam Database Lookup Results for 66.216.133.29

rDNS/PTR record for 66.216.133.29 is "mail1.trump-email.com".

Some mail servers will not accept mail from IP addresses with no rDNS/PTR record or a generic PTR record.

The following are blacklist test results. Being listed with a DNSBL does not always indicate the IP address is a source of spam. Some DNSBL's criteria are based of the IP address' country or connection type. If you are listed with a DNSBL click on the link for removal criteria.

all.s5h.net	b.barracudacentral.org	bl.emailbasura.org
bl.spamcannibal.org	bl.spamcop.net	blacklist.woody.ch
bogons.cymru.com	cbl.abuseat.org	cdl.anti-spam.org.cn
combined.abuse.ch	db.wpbl.info	dnsbl-1.uceprotect.net
dnsbl-2.uceprotect.net	dnsbl-3.uceprotect.net	dnsbl.anticaptcha.net
dnsbl.cyberlogic.net	dnsbl.dronebl.org	dnsbl.inps.de
dnsbl.sorbs.net	dnsbl.spfbl.net	drone.abuse.ch
duinv.aupads.org	dul.dnsbl.sorbs.net	dyna.spamrats.com
dynip.rothen.com	exitnodes.tor.dnsbl.sectoor.de	http.dnsbl.sorbs.net
ips.backscatterer.org	ix.dnsbl.manitu.net	korea.services.net
misc.dnsbl.sorbs.net	noptr.spamrats.com	orvedb.aupads.org
pbl.spamhaus.org	proxy.bl.gweep.ca	psbl.surriel.com
relays.bl.gweep.ca	relays.nether.net	sbl.spamhaus.org
short.rbl.jp	singular.ttk.pte.hu	smtp.dnsbl.sorbs.net
socks.dnsbl.sorbs.net	spam.abuse.ch	spam.dnsbl.anonmails.de
spam.dnsbl.sorbs.net	spam.spamrats.com	spambot.bls.digibase.ca
spambl.imp.ch	spamsources.fabel.dk	ubl.lashback.com
ubl.unsubscore.com	virus.rbl.jp	web.dnsbl.sorbs.net
wormbl.imp.ch	xbl.spamhaus.org	z.mailspike.net
zen.spamhaus.org	zombie.dnsbl.sorbs.net	

(c) ***Records Indicate "Mail1.trump-email.com" Was Not Sending Automated Bulk/Marketing Emails:*** Because DNS records have time stamps with precision down to the second, it is possible to identify patterns in DNS records. For example, if a server is processing marketing or bulk emails, there will be regular high-volume DNS look-ups, followed by low volume periods (an email is sent to thousands/millions of users, and then the email server is dormant before sending an email to thousands/millions of users again).[111] Conversely, in human-driven email-type message delivery or communications, the DNS look-ups would likely reflect a much lower volume of DNS look-ups, with a pattern of look-ups associated with typical non-bulk email exchanges: quick replies in some cases, and slight delays in others. A statistical analysis of the timing of the "**mail1.trump-email.com**" DNS look-ups by **Alfa Bank** and **Spectrum Health** found that the inter-arrival times (the time space between DNS look-ups that may precede an email being delivered) are not consistent with automated, bulk email.[112]

Additional supporting evidence indicating that "**mail1.trump-email.com**" was not operating as a marketing or bulk email server can be found in the technical attachment.

---

[110] Using the site: http://www.dnsbl.info/dnsbl-database-check.php

[111] As described in this memo, the lack of a SPF authorization record associated with "mail1.trump-email.com" significantly complicates the use "mail1.trump-email.com" for marketing or bulk email.

[112] See "Time Series Analysis" attachment (based on third-party data) which describes the pattern of DNS look-ups reflecting typical human-based email exchanges. In the attachment, a third-party researcher calculates the inter-arrival time between DNS look-ups for "mail1.trump-email.com" using a simple time series analysis. As would be expected, spam, viruses, bulk newsletter emails, and marketing emails exhibit less "back-and-forth." Put another way, people rarely reply to marketing emails, bulk newsletters, or spam. Conversely, people frequently respond to emails directly addressed to them and personalized. The data detailed in the attachment identifies the DNS look-ups as reflecting human-driven interactions that is not consistent with automation, backups, or infectious behavior.

In summary, the **Trump Organization** appropriately maintained an SPF authorization record for its servers that were authorized to send official email from "trump-email.com." This SPF Record did not include "**mail1.trump-email.com**." Some email providers, including some large Fortune 500 companies, are configured to refuse incoming email if the SPF authorization fails.[113] For these reasons, "**mail1.trump-email.com**" would not have been an effective means to send marketing or bulk email. Further, had "**mail1.trump-email.com**" been sending marketing or bulk emails, the IP address sending those bulk emails would likely appear in public spam block lists. With the exception of one block list that rejects email without SPF authorization records, the IP address for "**mail1.trump-email.com**" does not appear. Based on these facts, it is unlikely that "**mail1.trump-email.com**" was being used to send marketing or bulk email during the period of interest. Finally, because DNS records have time stamps with precision down to the second, it is possible to identify patterns in DNS records. The pattern of DNS look-ups for "**mail1.trump-email.com**" was found not to be consistent with automated, bulk email.

[113] Per Internet Engineering Task Force guidance, most organizations will accept mail with a "softfail" SPF record like the referenced Trump Organization server SPF entry. The email, however, is likely to be filtered to spam or promotional folders rather than delivered directly to an inbox.

Finding #4

4. **Testing indicates that the server assigned to the Trump Organization ("mail1.trump-email.com") was configured to accept email.** [114]

Research indicates that "**mail1.trump-email.com**" was running an email server and was accepting connections on Port 25, the server port dedicated to email.[115]

When a third-party researcher used *Pingability* (a server and website monitoring and alert service) to open a connection (essentially sending a test email) to Port 25 of "**mail1.trump-email.com**," the researcher found that "**mail1.trump-email.com**" was correctly running SMTP software (Simple Mail Transfer Protocol, the protocol used to exchange email on the internet).

The following error was received by the researcher: "*521 lvpmta14.lstrk.net does not accept mail from you.*" This error message reveals:

- "521": This response code means that the server will not accept email on the testing incoming connection.[116]
- "lstrk.net": This response code means the connection is being made to a Listrak server.[117]
- "does not accept mail from you": This response code means the server would not accept the test email.

This test reveals that either the server was configured to reject email from everyone, or that the server was configured to accept only emails from specific senders. The SMTP software associated with Listrak, "Port25 powerMTA," is a commercial SMTP software which offers an "access control list" (ACL) capability. This would permit the Trump Organization server, "**mail1.trump-email.com**," to filter out connections and emails based on their originating IP address and accept email only from approved parties. In this case, it's possible that "**mail1.trump-email.com**" was configured to only permit connections from specific entities (IP addresses). Given the DNS look-ups, those entities (IP addresses) could be Alfa Bank, Spectrum Health, and

[114] As described in the technical attachment, this finding does not lead our researchers to conclude that the server was exchanging traditional email. In fact, the lack of MX or TXT queries makes it highly unlikely that these four entities were sending ordinary SMTP email amongst themselves. Nonetheless, the DNS data overwhelming points to the fact that there was a special communications relationship between the four entities discussed in this memorandum during the period of interest. In other words, whatever the purpose of the server named "mail1.trump-email.com" during the period of interest, that purpose was something almost exclusively used by Alfa Bank, Spectrum Health, and to a lesser extent, Heartland Payments Systems.

[115] The mail server may not have been the only application or program running on the server. Indeed, there are some indications that the server may have included a program that allowed for other types of communication outside of email. For example, reporting indicates that Cendyn's Metron meeting software and CendynOne Customer Relations Management system were deployed on this server.
See attachments for additional information.
See https://port25.com/case-study-email-service-provider-listrak/

[116] Foundational Technical Standard RFC 1846.

[117] Listrak is a Lititz, Pennsylvania, company that sends marketing and bulk emails on behalf of corporate clients, including the Trump Organization during the period examined. For more information, see Appendix. http://lancasteronline.com/news/local/fbi-gets-lititz-firm-s-help-in-probe-of-russian/article_ef5d5ed0-05ae-11e7-a003-471e5543b26a.html

Heartland Payment Systems—as these are the only entities (IP addresses) conducting continued DNS look-ups for the Trump Organization server.

Finding #5

5. The data indicates that in September 2016 there was likely human interaction and coordination between personnel working on behalf of Alfa Bank (or their designees) and personnel working on behalf of the Trump Organization (or their designees).

Note: *In this section, analysis is provided of DNS records generated after September 21, 2016, which earlier in this memorandum is described as the end date for the DNS data-set analyzed in other sections. As this section explains, the additional DNS records from after September 21, 2016, are unlike those that precede them. Prior to September 21, 2016, the DNS records by cadence indicate human-directed communications. After this date, a human-directed event (the deletion of the zone "**trump-email.com**") that resulted in severing the server connections produced a surge of automated computer activity trying to reestablish those connections.*

Some of the information on the unusual DNS activity described in this memo was provided to *The New York Times* in late summer 2016. As part of its investigative efforts, *The New York Times* contacted representatives of Alfa Bank on September 21, 2016, and asked for an explanation for the abnormal communications behavior between Alfa Bank servers and a server assigned to the Trump Organization.[118]

On September 23, 2016, two days after *The New York Times* approached Alfa Bank, the Trump Organization deleted the email server "**mail1.trump-email.com**" (the server was first registered to the Trump Organization on August 14, 2009.[119])[120] In technical terms, the "A" record (i.e. the name) was deleted. The deletion of the "A" record for the server ("**mail1.trump-email.com**") on the Trump Organization network would not have been automated, rather it would have been a deliberate human action taken by a someone working on behalf of the Trump Organization and *not by Alfa Bank*. An analyst, quoted in the *Slate* article by Franklin Foer, observed that "*the knee was struck in Moscow, and the leg kicked in New York.*"[121]

When the Trump Organization deleted the "A" record for this Trump Organization server, any attempt to communicate with the server would fail. DNS records reveal that immediately after "**mail1.trump-email.com**" was deleted, the servers associated with Alfa Bank and Spectrum Health repeatedly attempted to do a DNS look-up of "**mail1.trump-email.com**," but the DNS look-up repeatedly failed, as the "A" record had been deleted.[122] (To continue the telephone

[118] http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html

[119] http://www.ljean.com/NetworkRecords/Trump-Owned-And-Mail-Systems-WHOIS-15.txt

[120] See http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html "The server was first registered to Trump's business in 2009 and was set up to run consumer marketing campaigns."

[121] http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html

[122] The DNS look-ups by Alfa Bank and Spectrum Health suggest that both were trying to reconnect to "mail1.trump-email.com" to reestablish communications.

analogy, there was no longer a phone number associated with the name of the business—as the phone number had been discontinued and disconnected. In this case, there was no longer an IP address associated with the server named "**mail1.trump-email.com**").

> **Note:** In addition to the surge in failed DNS look-ups for "**mail1.trump-email.com**" from the Alfa Bank and Spectrum Health servers , there were observed failed DNS look-ups originating from a new Alfa Bank IP address (217.12.97.137) seeking the name "mail.trump-email.com.moscow.alfaintra.net" for a period of 5-6 minutes.[123] The DNS look-ups begin at 2016-09-23T13:50:50 (starting 2 minutes and 44 seconds after the last successful DNS look-up for "**mail1.trump-email.com**") and end at 2016-09-23T13:56:29. These DNS look-ups were not seen previously in the data and are never seen again outside of this 5-6 minute period.[124] The timing of the DNS look-ups by this new IP address associated with Alfa Bank coincide exactly with the deletion of the "A" record by a representative of the Trump Organization.[125]

The last successful DNS look-up of "**mail1.trump-email.com**" was by Alfa Bank on September 23, 2017, at 13:48:06hrs UTC. The first DNS look-up for "**mail1.trump-email.com**" that failed was by Spectrum Health on September 23, 2017, at 14:11:40hrs UTC.

Entry	Time Stamp (UTC)	IP Address	DNS Look-Up	Result
3739	2016-09-23T13:48:06	217.12.96.15 (Alfa Bank)	mail1.trump-email.com	RCODE:No Error
3750	2016-09-23T14:11:40	167.73.110.8 (Spectrum Health)	mail1.trump-email.com	RCODE:Server Failure

[123] Data-set entitled "DNSLUPSMAIL1082417." This was likely a mistyped address by a human on the Alfa Bank network.
[124] Data-set entitled "DNSLUPSMAIL1082417." Per a third-party analysis: [REDACTED-[redacted](@[redacted]] registered a dynamic DNS record that points to 217.12.97.137.
[125] See also http://www.ljean.com/NetworkRecords/intranet/index.html; Intra Net DNS Leakage explanation by J. Camp. A summary of the analysis by Dr. Camp explains: An intranet is a company's internal network, intra or inside the boundaries of the company. Intranets are not intended to be accessible or visible from the outside except via special access. These private networks are for business and are not publicly accessible. Such networks run off a green list or white list of approved parties. DNS leakage does occur occasionally between a company's internal network and the internet due to errors and misconfigurations. Here we see clear indication that the Moscow division of the INTERNAL Alfa Bank network most definitely has purposeful communications with a hostname registered by the Trump Organization. The concatenation below is a DNS leak of an internal configuration. If a machine were spamming a company, you would block it. You would be highly unlikely to change your internal intranet records to make sure the connection continued. Here we see a change to the Trump-Email.com zone from DNS by Cendyn. (Cendyn has stated that the host was indeed in use for "a bank" that wanted to have "meetings" with Alfa Bank). This query is unusual in that it merges two hostnames into one. It makes the most sense as a human error in inserting a new hostname in some dialog window, but neglected to hit the backspace to delete the old hostname. Of course, this run-on hostname doesn't exist; it's just two hostnames run together. Some 90 seconds later, the networks stopped talking about this host (at 2016-09-23T13:56:29.000Z), and further queries were not seen. But the brief minute life of the query associates the trump-email server to a new zone: the Alfa Bank intranet network. The moscow.alfaintra.net is the internal LAN of Alfa Bank. Like most careful organizations, the bank intranet is only resolved and reachable via a VPN (or by being inside the Bank's network of course). The internal LAN network contains ldap servers, a Microsoft Active Directory server, a HipChat server, a few Apple Caching Servers, some Microsoft Key Management Service (KMS) systems, etc. The hybrid hostname suggests that Alfa was attempting to accommodate the Trump host in its network. After the 90-second "fat finger" event, the queries ceased as the record was corrected, and the targeted domain entered correctly.

After the "A" record was deleted for "**mail1.trump-email.com**" on September 23, 2016, Alfa Bank and Spectrum Health continued to conduct DNS look-ups for "**mail1.trump-email.com**." The response to these DNS look-ups indicated that there was no longer a server named "**mail1.trump-email.com**." In the case of Alfa Bank, this behavior persisted until late Friday night, on September 27, 2016 (Moscow time).[126] At that point, Alfa Bank ceased its DNS look-ups of "**mail1.trump-email.com**." Less than ten minutes later (2016-09-27T19:48:55), a server assigned to Alfa Bank was the first source in the DNS data-set (37 million DNS records from January 1, 2016, to January 15, 2017) to conduct a DNS look-up for the server name "trump1.contact-client.com."[127] The answer received was 66.216.133.29, the same IP address used for "**mail1.trump-email.com**" that was deleted in the days after *The New York Times* inquired with Alfa Bank about the unusual server connections. No servers associated with Alfa Bank ever conducted a DNS look-up for "trump1.contact-client.com" again, and the next DNS look-up for "trump1.contact-client.com" did not occur until October 5, 2016 (2016-10-05T18:11:03). Three of these five look-ups from October 2016 originated from Russia (*see* chart below).

	Date	IP Address	DNS Look-Up	ASN	Entity	Reverse DNS Name of IP
1	2016-09-27T19:48:55	217.12.97.15	**trump1.contact-client.com**	15632	ALFA-BANK-AS, RU	ns2.alfadirect.net
2	2016-10-05T18:11:03	203.109.188.30	**trump1.contact-client.com**	9500	VODAFONE-TRANSIT-AS NZ Ltd., NZ	akl-ftc-mrdns1.ihug.net
3	2016-10-05T18:11:03	203.89.226.26	**trump1.contact-client.com**	9328	DATACOM-AU Datacom, AU	mdbs2.globalcenter.net.au
4	2016-10-10T17:13:49	91.205.144.100	**trump1.contact-client.com**	47923	LANCRAFT-AS, RU	[Errno 1] Unknown host
5	2016-10-10T17:13:51	91.205.144.100	**trump1.contact-client.com**	47923	LANCRAFT-AS, RU	[Errno 1] Unknown host

[126] The DNS look-ups for "mail1.trump-email.com" from Spectrum Health rapidly continued until September 30, 2017, at 16:15 (UTC), only to appear one last time on December 14, 2016, at 18:37 (UTC).

[127] Cendyn controls the domain name "contact-client.com." See http://whois.domaintools.com/contact-client.com. Charles Deyo is the CEO of Cendyn. "Domain Name: CONTACT-CLIENT.COM Registrar URL: http://www.godaddy.com Registrant Name: Charles Deyo Registrant Organization: Name Server: NS3.CDCSERVICES.COM Name Server: NS2.CDCSERVICES.COM Name Server: NS1.CDCSERVICES.COM DNSSEC: unsigned"

	Date	IP Address	DNS Look-Up	ASN	Entity	Reverse DNS Name of IP
6	2016-10-10T17:14:21	91.205.144.100	**trump1.contact-client.com**	47923	LANCRAFT-AS, RU	[Errno 1] Unknown host

Sometime between November 11, 2016, and November 28, 2016, the "A" record for this server, "trump1.contact-client.com," was also deleted.[128] There are no DNS records indicating **Spectrum Health** ever conducted a DNS look-up for "trump1.contact-client.com."

The fact that Alfa Bank was the first entity (IP address) to conduct a DNS look-up for "trump1.contact-client.com" in the data-set could indicate that someone at Alfa Bank was in some manner made aware of the new Trump Organization server name.[129] To continue the telephone analogy, it is as if a person at the Trump Organization created a new unlisted telephone number, and shortly thereafter, the first incoming call received was from Alfa Bank, the most frequent caller of the old telephone number. Put another way, the only way Alfa Bank would have known to *"call the telephone number,"* was if it was informed what number to call. Thus, to use the analyst's analogy previously referenced, this time, the reflex action was reversed: the knee was struck in the Trump Organization in New York (the deletion of the server), and the leg kicked in Alfa Bank in Moscow (the look-up of the new Trump Organization server).

[128] See data-set entitled "DNSLUPSMAIL1082417," where "trump1.contact-client.com" begins to appear as "non-existent domain."

[129] The first DNS look-up could have been generated by an Alfa Bank Information Technology employee reconfiguring a mail server, or it could have been any user at Alfa Bank addressing a new email to a user at "trump1.contact-client.com."

TIMELINE

- 2009 – "Mail1.trump-email.com" is registered on behalf of the Trump Organization on August 14, 2009, to manage consumer marketing campaigns by Cendyn, a third-party vendor.[130]
- March 2016 – Cendyn claims to send the last marketing email for the Trump Organization.[131] Cendyn's contract with the Trump Organization is replaced by Serenata, a German email marketing company who states that it never used "mail1.trump-email.com."[132]
- May 2016 through September 2016 – During this period, "mail1.trump-email.com" is regularly, and almost exclusively, communicating with Alfa Bank, Spectrum Health, and Heartland Payment Systems.[133]
- September 21, 2016 – As part of an investigation, *The New York Times* contacts representatives of Alfa Bank and asks for an explanation for the unusual communications between the Alfa Bank servers and "mail1.trump-email.com."[134]
- September 23, 2016 – Two days after *The New York Times* approaches Alfa Bank, the Trump Organization deletes the "A" record for "mail1.trump-email.com," which was initially registered to the Trump Organization in 2009 (this deletion occurred prior to any approach by *The New York Times* to the Trump Organization).[135]
- September 27, 2016 – A server assigned to Alfa Bank is the first entity (IP address) in the DNS data-set to conduct a DNS look-up for a server named "trump1.contact-client.com." The answer received is 66.216.133.29, the same IP address previously used for "mail1.trump-email.com."[136]
- November 2016 – The "A" record for "trump1.contact-client.com" is deleted.[137]

---

[130] http://www.ljean.com/NetworkRecords/Trump-Owned-And-Mail-Systems-WHOIS-15.txt

[131] https://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/

[132] https://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/
Serenata Intraware GmbH is a German marketing company based in Munich, Germany, and San Francisco, California. Founded in 1996 and led by CEO Johann Deil, Serenata identifies as "one of the foremost authorities on [customer relationship management (CRM)] technology in the world." https://www.worldtravelawards.com/news-2442. On September 17, 2015, Serenata announced that Trump Hotel Collection selected Serenata as its CRM partner "to deliver the integrated, seamless solutions required to meet Trump's unwavering standard of excellence." https://www.hospitalitynet.org/news/4071796.html

[133] Data-set entitled "DNSLUPSMAIL1082417."

[134] http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html

[135] http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html

[136] Cendyn controls the domain name "contact-client.com." See http://whois.domaintools.com/contact-client.com. Charles Deyo is the CEO of Cendyn. "Domain Name: CONTACTCLIENT.
COM Registrar URL: http://www.godaddy.com Registrant Name: Charles Deyo Registrant Organization: N
ame Server: NS3.CDCSERVICES.COM Name Server: NS2.CDCSERVICES.COM Name Server: NS1.CDCSERVICES.COM
DNSSEC: unsigned"

[137] See data-set entitled "DNSLUPSMAIL1082417," where "trump1.contact-client.com" begins to appear as "nonexistent domain."

In summary, two days after *The New York Times* approached Alfa Bank about itsunusual connections to "**mail1.trump-email.com**," someone working on behalf of the Trump Organization deleted the name of the server that had been the subject of the DNS look-ups by Alfa Bank, Spectrum Health, and Heartland Payment Systems. The first entity (IP address) in the DNS data-set (37 million DNS records from January 1, 2016, to January 15, 2017) to conduct a DNS look-up for "trump1.contact-client.com," associated with the same IP address (66.216.133.29), was a server associated with Alfa Bank.

The deletion of "**mail1.trump-email.com**" was a human action, not automated. Similarly, the initial DNS look-up by the Alfa Bank server of "trump1.contact-client.com" was likely the result of human input and interaction.

Finding #6

6. **The Alfa Bank funded-investigations by Stroz Friedberg (*overseen by Brian Benczkowski, the current Assistant Attorney General of the Criminal Division at the Department of Justice*) and Mandiant do not refute the allegations made regarding the server connections, or the findings of this memo.**

On June 5, 2017, President Trump announced his intention to nominate **Brian Benczkowski** to be Assistant Attorney General for the Criminal Division of the Department of Justice.[138] **Benczkowski** had previously served on the **Trump Administration Transition Team**.

Benczkowski has a longstanding relationship with Attorney General **Jeff Sessions**, having previously served as Staff Director for then-Sen. Sessions after Sessions was named Ranking Member of the **Senate Judiciary Committee** in 2009.[139] Benczkowski joined Donald Trump's transition team in September 2016 and led the transition team for the Justice Department before returning to private practice after the 2017 presidential inauguration.[140]

In March 2017, as a lawyer at Kirkland & Ellis, **Benczkowski** oversaw an investigation commissioned by **Alfa Bank** into the **Alfa Bank** server connections to a Trump Organization server.

In July 2017, in advance of his Senate nomination hearing, **Benczkowski** submitted materials to the **Senate Judiciary Committee** on two investigations[141] commissioned by **Alfa Bank**. The first is a November 4, 2016, investigative report marked "*draft*" by **Mandiant**. The second report, overseen directly by **Benczkowski**, was conducted by **Stroz Friedberg** and dated July 19, 2017.

Benczkowski testified that **Mandiant** "*looked at the 2016 allegations and found them to be inaccurate. And there to be nothing to it*."[142] However, a July 24, 2017, *New York Times* article provided a different description of the report, stating:

> *"According to people familiar with **Mandiant's** review, its experts were shown largely metadata, the information that travels along with a message, for the communications that took place. The contents of the messages — if there were any — were not available. Without a much deeper forensic examination, the*

[138] https://www.whitehouse.gov/the-press-office/2017/06/05/president-donald-j-trump-announces-intent-nominate-personnel-key

[139] http://www.cnn.com/2017/07/24/politics/brian-benczkowski-alfa-bank/index.html; http://politicalticker.blogs.cnn.com/2009/05/13/sessions-announces-judiciary-staff/; https://www.washingtonpost.com/news/powerpost/wp/2016/11/16/brian-benczkowski-once-dubbed-gops-go-to-guy-for-hearings-helping-manage-justice-department-transition/?utm_term=.80ce743c5faa

[140] https://www.feinstein.senate.gov/public/index.cfm/press-releases?id=71649645-8A75-4C9A-8C45-8CEA26A4D4B7

[141] The Mandiant report stated that they conducted their review "in conjunction with Alfa-Bank," that they relied entirely on information provided by Alfa Bank, and that the material necessary to conduct a review of the 2016 server allegations was unavailable. The Stroz Friedberg similarly stated it could not review the 2016 allegations because Alfa Bank did not preserve the required information, stating the data "no longer exists" at Alfa Bank. See http://i2.cdn.turner.com/cnn/2017/images/07/24/dinh.to.grassley.feinstein.pdf

[142] Senate Judiciary Confirmation Hearing for the nomination of Brian Allen Benczkowski, to be an Assistant Attorney General, Criminal Division, Department of Justice, July 25, 2017. https://www.judiciary.senate.gov/imo/media/doc/Benczkowski%20Responses%20to%20QFRs.pdf.

company could not determine the purpose of the communications. Its resulting report was carefully hedged, noting that without more study, it could not give the bank a clean bill of health. But the bank used that report, however limited, to make the case that it had been exonerated."[143]

(a) ***Mandiant Report:*** The 14-page **Mandiant** report [*including cover (page 1), table of contents (page 2), and numerous images and exhibits*] states on page 8 that **Mandiant** did not have access to the necessary DNS records to complete their investigation:

> *"At the time **Mandiant** initiated their investigation, **Alfa-Bank**'s log retention was set to 24 hours. **Alfa-Bank** indicated this was due to normal operations generating a high volume of requests; therefore, physical space for log storage was not economically feasible"*[144]

Without access to the necessary data, **Mandiant** explored the possibility that "trump-email.com" had been used for marketing or bulk email purposes and that a security software tool may have been responsible for the **Alfa Bank** DNS look-ups of "**mail1.trump-email.com**" in response to such emails.[145]

The **Mandiant** report details how *"in conjunction with Alfa-Bank,"* they observed that **Alfa Bank** security software (Trend Micro Deep Discovery Inspector) would conduct a DNS look-up of all domain names mentioned in the bodies of the emails received to determine whether they were malicious. They tested this by sending a *"fictitious"* domain name ("dns-servertrump-email.com") and found that this "caused 11 automated DNS requests" (these DNS requests included "A and AAAA requests," two different types of DNS requests).[146]

The **Mandiant** report is careful not to state that the referenced security software caused the **Alfa Bank** DNS look-ups of "**mail1.trump-email.com**;" (however, the reader can be left with that impression due to the how the report is structured.) After discussing the **Alfa Bank** security software (Trend Micro Deep Discovery Inspector) Mandiant's report states it *"investigated how the 'trump-email.com' domain was used in the past,"* and found that *"the domain formerly offered hotel promotion deals for a Trump hotel."*[147] The report states that **Mandiant** searched 12-months of email archives provided by **Alfa Bank** and was able to locate three marketing email hits for "**mail1.trump-email.com**." However, all three emails were sent prior to February 5, 2016, and therefore were not germane to the

[143] https://www.nytimes.com/2017/07/24/us/politics/brian-benczkowski-justice-alfa-bank.html?mcubz=1
[144] See Mandiant Report Page 8, http://i2.cdn.turner.com/cnn/2017/images/07/24/dinh.to.grassley.feinstein.pdf. Note: The Mandiant Report asserts that Alfa Bank began retaining DNS records after October 2016.
[145] As detailed in this report, the server was not being used for marketing purposes during the period in question.
[146] As a further refutation of the Mandiant report, there are no AAAA DNS requests in the DNS records from May 4, 2016, to September 21, 2016. If the Alfa Bank security software was responsible for the Alfa Bank DNS look-up of the Trump Organization server, based on Mandiant's testing and hypothesis, there would be AAAA DNS look-ups in the data collected. Moreover, it would be exceptionally odd for the Trump Organization server to be just sending marketing email repeatedly to just Alfa Bank, Spectrum Health, and Heartland Payment Systems.
[147] See Mandiant Report, page 11.

time period in question (This finding is congruent with the assertions of **Cendyn**, which told CNN that the company ceased email marketing operations for the **Trump Organization** in March 2016.).[148]

There are three key issues with the **Mandiant** report:

- First, the test conducted by **Mandiant** of the **Alfa Bank** security software (Trend Micro Deep Discovery Inspector) used a "*fictitious*" domain name and found it "caused 11 automated DNS requests." However, "**mail1.trump-email.com**" was an actual domain name (not fictitious), and there is no indication or test of how many, if any, DNS requests would occur if a real domain name was used to conduct a comparable test.

- Second, between May 4, 2016, and September 21, 2016, there were **2,761 Alfa Bank DNS look-ups** for "**mail1.trump-email.com**." **Mandiant** states they found only three marketing emails from "**mail1.trump-email.com**" in the email archives of **Alfa Bank** (retained from the preceding 12 months). Mandiant could find no emails during the period of time in question. Moreover, by Mandiant's own calculations – the three emails produced would only have accounted for approximately 33 DNS look-ups of "**mail1.trump-email.com**," not 2,761 look-ups.

- Third, the three emails referenced could not be responsible for any of the **2,761 Alfa Bank DNS look-ups** for "**mail1.trump-email.com**," as these emails were found to have been sent significantly before the date range in question, May 4, 2016, to September 21, 2016 (nothing after March 2016).

In conclusion, the **Mandiant** report acknowledges that **Alfa Bank** could not provide the DNS records needed to review the **Alfa Bank** DNS look-ups for the Trump Organization server from May 4, 2016, to September 21, 2016. While **Mandiant** then indicates that marketing email could have caused the Alfa Bank security software to conduct a limited number of DNS look-ups, Mandiant and Alfa Bank could not produce any marketing email from the **Trump Organization** during the period in question to support the theory, nor could Mandiant account for the volume of DNS look-ups.

(b) ***Stroz Friedberg Investigative Report***: The Alfa Bank-funded **Stroz Friedberg** 6-page investigative report [*including cover (page 1), a table of contents (page 2), and a promotional closing (page 6)*] states on page 3 that the company was unable to assess the allegations pertaining to the 2016 server communications between Alfa Bank and the Trump Organization because of a lack of data:

[148] http://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/index.html; http://i2.cdn.turner.com/cnn/2017/images/07/24/dinh.to.grassley.feinstein.pdf; One of the three emails is from 2015, the remaining two are from February 2016.

> *"However, because the information is from 2016 (when Alfa-Bank's practice was to preserve DNS log data only for 24 hours), log data at the bank no longer exists for that timeframe. As such, we were unable to verify whether or not the information is valid."*

Notwithstanding **Stroz Friedberg**'s acknowledgement that they could not assess the 2016 allegations, **Benczkowski** testified that **Stroz Friedberg** "*communicated directly with the bank to get the information that they needed to conduct their review*" and that "*Stroz Friedberg found that there, once again, was no communication link between the Trump Organization and Alfa Bank.*"[149]

The **Stroz Friedberg** report suggests there were allegations that the server connections between **Alfa Bank** and the **Trump Organization** continued in 2017. A comprehensive search of news and blog posts from October 31, 2016 (when the original story was detailed in *Slate*) to August 30, 2017, uncovered no claims that Alfa Bank and Trump Organization servers were communicating in 2017.[150] Notwithstanding the lack of allegations, the materials submitted by **Benczkowski** to the Senate state that Stroz Friedberg's investigation "*found no evidence of any connections or communications between Alfa-Bank and the Trump Organization occurring in 2017.*"[151] As per the above, the only serious allegations of communications between **Alfa Bank** and the **Trump Organization** pertain to 2016, not 2017.[152]

[149] Senate Judiciary Confirmation Hearing for the nomination of Brian Allen Benczkowski, to be an Assistant Attorney General, Criminal Division, Department of Justice, July 25, 2017. https://www.judiciary.senate.gov/imo/media/doc/Benczkowski%20Responses%20to%20QFRs.pdf.
[150] Search conducted October 2017.
[151] http://i2.cdn.turner.com/cnn/2017/images/07/24/dinh.to.grassley.feinstein.pdf
[152] While the Stroz Friedberg report states, "[m]ultiple news articles and blog posts speculated that these 2016 and 2017 DNS queries are indicative of communication between Alfa-Bank and The Trump Organization," no reputable allegations could be found contending there was any communication between the Trump Organization Server and the Alfa Bank server in 2017.

Finding #7

7. The public statements by the Trump Organization, the Trump Campaign, Spectrum Health, and Alfa Bank on the server connections are contradictory and omit pertinent facts. Heartland Payment Systems has never commented on its server connections to the Trump Organization server.[153]

The parties who have commented on the alleged server allegations have offered varying and contradictory statements:[154]

(a) ***Alfa Bank***: In October 2016, a representative for Alfa Bank, Barbour, Griffith, & Rogers (BGR), a U.S. based lobbying and public relations firm, told *Slate Magazine* that "*neither Alfa Bank nor its principals, including Mikhail Fridman and Petr [Pyotr] Aven, have or have had any contact with Mr. Trump or his organizations.*"[155] The representative added that Alfa Bank and its officers have not "*sent Mr. Trump or his organizations any emails, information or money*" and that the "*assertion of a special or private link is patently false*."[156]

Months later, in March 2017, Alfa Bank released a statement that seemed to confirm their servers were in contact with a server from the Trump Organization. In a CNN article published on March 8, 2017, Alfa Bank commented on the "*server communication*" stating that "*the most likely explanation is that the server communication was the result of spam marketing*" from the Trump Organization. Alfa Bank noted that company executives "*have stayed at Trump hotels, so it's possible they got subsequent spam marketing emails from the Trump Organization.*"[157] Per Alfa Bank, "*[t]hose emails might have set off defensive cybersecurity measures at the bank, whose servers would respond with a cautious DNS lookup.*"[158] Alfa Bank added that it "*used antispam software from Trend Micro, whose tools would do a DNS lookup to know the source of the spam.*"[159]

Alfa Bank has also suggested in letters to Indiana University Professor and DNS expert Dr. L. Jean Camp that the DNS records may have been fabricated, while also indicating that the DNS records were improperly acquired from Alfa Bank.[160]

(b) ***Cendyn & Serenata***: Both Cendyn and Serenata have denied utilizing the Trump Organization server for email marketing after March 2016. In response to the

[153] See chart of public statements in attachments.
[154] See technical attachment for detailed refutations of these statements.
[155] http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html
[156] http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html
[157] http://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/
[158] http://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/
[159] http://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/
[160] ljean.com/files/AlfaBankLetter2.pdf

aforementioned October 31, 2016, *Slate Magazine* article, the Trump Organization called on Cendyn, a third-party vendor that operated the "**mail1.trump-email.com**" server on its behalf, to conduct an analysis of the alleged server connections.[161] In November 2016, Cendyn confirmed there was a server connection, but reported that an "*existing banking customer of Cendyn, completely unrelated to Trump, recently used Cendyn's 'Metron' Meeting Management Application to send communication [sic] to AlfaBank.com.*"[162] On multiple occasions, including on March 2017, Cendyn stated that its contract to provide email marketing services to the Trump Organization ended in March 2016—prior to the period in question—with the Trump Organization hiring Serenata, a German email marketing company, to replace them.[163] In March 2017, Serenata told CNN that it was hired by Trump Hotels, but that it "never has operated or made use of" the server "**mail1.trump-email.com**."[164]

(c) ***Spectrum Health***: In October 2016, Spectrum Health stated that after conducting a "*rigorous*" investigation, the company did not find "*actual communications (no emails, chat, text, etc.) between Spectrum Health and Alfa Bank or any of the Trump organizations.*"[165] Spectrum Health then stated in March 2017 that it found a "'*small number of incoming spam marketing emails' from 'Cendyn, advertising Trump Hotels,*'" that occurred in 2015. As noted, this is before the period in question.[166]

On March 17, 2017, **Alfa Bank**, through a press release, stated that it was the victim of at least three "*DNS attacks*" in February and March 2017 by hackers intending "*to make it seem as if the Trump Organization is currently communicating*" with the bank.[167] Computer experts and journalists did not appear to agree with Alfa Bank's statement, and our researchers could not locate any reports of individuals claiming that the "*DNS attacks*" indicated a 2017 connection between the Trump Organization and Alfa Bank.[168]

As of September 1, 2018, **Heartland Payment Systems** has never publicly commented on its connections to the Trump Organization server.

---

[161] http://www.complex.com/life/2016/11/donald-trump-server-communicating-with-russia
[162] http://www.complex.com/life/2016/11/donald-trump-server-communicating-with-russia
[163] http://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/ Serenata Intraware GmBH is a German marketing company based in Munich, Germany, and San Francisco, California. Founded in 1996 and led by CEO Johann Deil, Serenata identifies as "one of the foremost authorities on [customer relationship management (CRM)] technology in the world." https://www.worldtravelawards.com/news-2442 In September 2015, Serenata announced that Trump Hotel Collection selected Serenata as its CRM partner "to deliver the integrated, seamless solutions required to meet Trump's unwavering standard of excellence." https://www.hospitalitynet.org/news/4071796.html
[164] http://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/index.html.
[165]http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html
[166] http://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/
[167] http://www.cnn.com/2017/03/17/politics/alfa-bank-trump-dns-hack/; https://alfabank.com/media/news/2017/03/17/
[168] Search conducted October 2017.

Appendix

Technical Attachment

Review of Claims Regarding "mail1.trump-email.com"

This attachment is intended for a reader with technical expertise.

Recap & Purpose

Several sources and informal collaborators have assembled a body of data about the behavior of a server named "mail1.trump-email.com" during 2016 and 2017. Several claims have been made about the meaning of this data in the media and web forums. This document attempts to neutrally analyze those claims based on direct access to the DNS data. The researchers and technical experts consulted for this memo include experts with knowledge of the theory and practice of administering DNS, SMTP, and TCP/IP networks. Our researchers spent more than twelve months examining the primary data, secondary documents, and all other available information.

Assumptions

The DNS data-set, which encompasses more than 37 million records, includes 27,390 queries for "trump-email.com" spanning the period from January 1, 2016, to January 15, 2017. The data-set, which was closely reviewed by researchers, is believed to be authentic. We further stipulate that these logs are a large, representative sample of all DNS traffic on the internet for this domain name during this period.

Examining these logs, our researchers found that the behavior during the period of May 4, 2016, to September 21, 2016, was strikingly different from the periods before and after. During these 141 days, significant traffic relating to the Trump Organization was observed from three entities: Alfa Bank, Spectrum Health, and Heartland Payment Systems. Hereafter, May 4, 2016, to September 21, 2016, will be referred to as the "*period of interest*."

Interpretations

The unusual DNS activity during the period of interest has an explanation; however, the DNS logs themselves cannot provide that explanation. The following are the two contrasting explanations that have been the most heavily promoted, and the technical observations that argue for and against each one.

Theory 1: The DNS Look-Ups are a Result of Spam Marketing Email

This theory says that the DNS look-ups of the Trump Organization server were merely a normal side effect of a large-scale spam/bulk email marketing campaign that Cendyn was

performing on behalf of Trump Organization – i.e., marketing email sent from the Trump Organization Server triggered many DNS look-ups to authenticate the email, or to check for malicious links in the body of the emails. This is the "*nothing to see here*" argument. Almost all technical observations argue that Theory 1 is false.

Evidence in Favor of Theory 1

- The domain was registered by Cendyn, an email marketing company, on behalf of the Trump Organization.
- Cendyn made a public statement that they conducted email marketing in the past on behalf of Trump hotels (but ended the practice in March 2016).[169]
- The Trump Organization made a public statement that they contracted with Cendyn for email marketing (but ended the practice in 2010).[170]
- When a researcher connected to port 25 on "**mail1.trump-email.com**" during the period of interest, the SMTP banner identified it as a "Listrak" email server.[171]

Evidence Against Theory 1

- The period of interest happened months after the end of the email marketing relationship between Cendyn and the Trump Organization, according to statements by both organizations.
- The number of unique source IP addresses resolving "**mail1.trump-email.com**" during the period of interest is very small and would reflect a marketing campaign to just three organizations: a Russian bank, a New Jersey payment processor, and a Michigan health care company. When our researchers looked at queries logged for the domain of a different Cendyn client, for example, there were more than a thousand sources.
- No examples of email sent containing "trump-email.com" during the period of interest have been produced, despite significant effort to find such emails (*see* Mandiant report).

[169] ttp://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/
[170] In the Slate Magazine piece from October 31, 2016, Hope Hicks stated that the Trump Organization server "has not been used since 2010." http://www.slate.com/articles/news_and_politics/politics/2016/11/the_trump_server_evaluating_new_evidence_and_countertheories.html
[171] Listrak is a Lititz, Pennsylvania, company that maintains servers to send marketing and bulk emails on behalf of corporate clients, including the Trump Organization. For more information, see http://lancasteronline.com/news/local/fbi-gets-lititz-firm-s-help-in-probe-of-russian/article_ef5d5ed0-05ae-11e7-a003-471e5543b26a.html

- The IP address for "**mail1.trump-email.com**" was not authorized to send email on behalf of "trump-email.com," according to the SPF record for that domain (which did exist).

- There were no "TXT" queries observed for "trump-email.com," which would have been generated if mail servers were receiving incoming email from "trump-email.com" and checking the SPF policy (Experimentation found that the mail servers for 20% of large corporations enforced SPF, including Alfa Bank.)

- A study of the intervals between query arrival times found that they were more suggestive of human activity than mass/bulk marketing email.[172]

- The DNS queries from Alfa Bank and Spectrum Health actually increased in frequency after the "**mail1.trump-email.com**" zone was deleted on September 23, 2016. It makes little sense for the operators to delete the zone, then increase the volume of email mentioning it.

- Servers used to send mass marketing email are typically found bouncing in and out of the more than a dozen published spam blacklists. A marketing company will work hard to keep out of blacklists, but regressions constantly happen. Our researchers did not see either the domain or the IP address in any of dozens of public blacklists.

Theory 2: The DNS Look-Ups Indicate There Was a Covert Email Server Side Channel

It has been claimed that "**mail1.trump-email.com**" was a "*secret email server*" that was used by the Trump Organization, Alfa Bank, and Spectrum Health. This theory fits many of the observations unexplained by the spam/marketing email theory, but is undermined by others.

Evidence in Favor of Theory 2

- The machine was named "**mail1.**"

- When a researcher attempted to connect to port 25 on "**mail1.trump-email.com**" during 2016, they found an SMTP banner, so an MTA was running there, at least.[173]

- The timing analysis showed heteroscedasticity that is a good fit for human two-way communication.[174]

[172] See Time Series Analysis in Appendix by third party.
[173] "*Port25 powerMTA,*" is a commercial SMTP software that offers an "*access control list*" (ACL) capability. This would permit the Trump Organization server, "mail1.trump-email.com," to filter out emails based on their originating IP address and only accept email connections from approved parties. See third-party analysis.
[174] See Time Series Analysis in Appendix by third party.

- The preponderance of DNS traffic coming from just four sources is overwhelming evidence that some special communication relationship existed among the four entities (two Alfa Bank servers, Spectrum Health, and Heartland Payment Systems). However, this evidence does not mean that the communication had to be conducted via email, or exclusively via email; other communication applications could have been used. In fact, researchers have confirmed that Cendyn offers its clients an array of services, including the ability to conduct communications and exchange payments.[175]

- The "**mail1.trump-email.com**" record was deleted (returning SERVFAIL) on September 23, 2016, which was two days after *The New York Times* contacted Alfa Bank. *The New York Times* did not contact representatives of Cendyn or the Trump Organization. It is either a coincidence, or *The New York Times* questions caused Alfa Bank to contact the Trump Organization, who then made changes to its domain.

- After the name was deleted, the query frequency from Alfa Bank dramatically increased on September 26, 2016, then the queries ceased altogether on September 27, 2016. The query frequency from Spectrum Health dramatically increased on September 23, 2016, and queries ceased on September 30, 2016. This would make sense if a mail relay was attempting delivery to "**mail1.trump-email.com**." Or it could indicate another type of application that conducted persistent reconnection attempts.

- For a period of 6 minutes immediately after the name was deleted, queries were logged from a different IP address at Alfa Bank, seeking "mail.trump-email.com.moscow.alfaintra.net." The concatenation of a target name with a local search domain can happen when a query fails, but nothing would automatically change the "mail1" component to "mail." After 6 minutes, these queries are never seen again, and nothing similar is seen from any other source in the world. Our researchers have no better theory than a human attempting to change something, while coordinating with administrators or representatives of the Trump Organization, given the precise timing.

- On September 27, 2016, ten minutes after Alfa Bank sent its last query for "**mail1.trump-email.com**," it sent the first query in the DNS data-set[176] for the qname, "**trump1.contact-client.com**." The domain resolved to the same IP address that used to be "mail1": 66.216.133.29. This is compelling evidence that someone provided "**trump1.contact-client.com**" to Alfa Bank for some communication purpose (although, again, this evidence does indicate the purpose was to send email).

[175] Preliminary research into Cendyn software services indicate that Cendyn provides clients with communications and payment sending capabilities via their eProposal and Guestfolio CRM software platforms.
[176] The 37 million DNS records from January 1, 2016, to January 15, 2017.

Evidence Against Theory 2

- The Trump Organization claimed there was no email communication, marketing or otherwise, between Alfa Bank and the Trump Organization.
- It would be unusual for the customer (Trump Organization) of an email marketing vendor (Cendyn or Serenata) to have sufficient control of the provisioned server to install different software and change its function on its own.
- There are no DNS queries of type "MX" in the logs, which would be expected if one simply tried to send an email in standard fashion to "someone@mail1.trump-email.com."[177]
- The SPF policy for "trump-email.com" did not include this machine.
- An attempt to talk to port 25 on "**mail1.trump-email.com**" was refused with an SMTP 521 message, "*this server does not accept mail from you*."

Inconclusive

- It could be argued that the lack of TXT queries (such as for the SPF policy) does not say much about a scenario where only four entities (IP addresses) are communicating, given the observation that only about one in five companies is enforcing SPF. However, third-party tests conducted during the period in question show that Alfa Bank consistently performed SPF/DKIM authentication look-ups, but not when querying the Trump server's DNS records.[178]

[177] https://www.eventhelix.com/RealtimeMantra/Networking/SMTP_Sequence_Diagram.pdf; See also, Address Resolution and Mail Handling, from RFC2821 (official authoritative direction from the Internet Engineering Task Force) regarding SMTP protocol: "Once an SMTP client lexically identifies a domain to which mail will be delivered for processing (as described in sections 3.6 and 3.7), a DNS lookup MUST be performed to resolve the domain name [22]. The names are expected to be fully-qualified domain names (FQDNs): mechanisms for inferring FQDNs from partial names or local aliases are outside of this specification and, due to a history of problems, are generally discouraged. The lookup first attempts to locate an MX record associated with the name. If a CNAME record is found instead, the resulting name is processed as if it were the initial name. If no MX records are found, but an A RR is found, the A RR is treated as if it was associated with an implicit MX RR, with a preference of 0, pointing to that host. If one or more MX RRs are found for a given name, SMTP systems MUST NOT utilize any A RRs associated with that name unless they are located using the MX RRs; the "implicit MX" rule above applies only if there are no MX records present. If MX records are present, but none of them are usable, this situation MUST be reported as an error. When the lookup succeeds, the mapping can result in a list of alternative delivery addresses rather than a single address, because of multiple MX records, multihoming, or both. To provide reliable mail transmission, the SMTP client MUST be able to try (and retry) each of the relevant addresses in this list in order, until a delivery attempt succeeds. However, there MAY also be a configurable limit on the number of alternate addresses that can be tried. In any case, the SMTP client SHOULD try at least two addresses."

[178] Additional Evidence that the Trump Organization Server was not Sending Traditional Email: If "mail1.trump-email.com" was being used for mail marketing purposes, recipient organizations would have made DNS queries to retrieve the SPF record to authenticate the email. However, the DNS records show no queries for the SPF text record – no type 16 text queries at all. Moreover, third-party tests conducted during the period in question show that Alfa Bank consistently performed SPF/DKIM authentication look-ups as a matter of practice. This provides additional evidence that the Trump Organization server was not sending marketing email.

Theory 3: The DNS Look-Ups Are Associated with Malware

It could be malware. But if the DNS look-ups are instead associated with malware or some infection vector, one would expect to see a more automated look-up pattern (Indeed, one would likely see the resolution of a 3rd party command-and-control domain, instead of basically three entities.). The lookup volume and paucity of qname diversity likely rules out this theory.

The problem with the malware hypothesis is that it could never be falsified. Even if malware caused the queries, the question remains: why are only these entities affected?

Conclusion

Our researchers conclude that Theory 1 (*The DNS Look-Ups are a Result of Spam Marketing Email*) is almost certainly false. Spam is nothing new on the internet, and mass mailings create easily observed phenomena, such as a wide dispersion of backscatter queries from spam filters. No such evidence is found in the logs.

Theory 2 (*The DNS Look-Ups Indicate There Was a Covert Email Server Side Channel)* is probably also incorrect for being too specific. The lack of MX or TXT queries makes it highly unlikely that these four entities were sending ordinary SMTP email. It would be an awkward and unusual configuration at best. Nonetheless, overwhelming evidence says that there was a special relationship between these four entities during the period of interest. **Whatever purpose the machine named "mail1.trump-email.com" served, that purpose was something nearly exclusively used by Alfa Bank, Spectrum Health, and Heartland Payments Systems**. Further, systems administrators for Alfa Bank and the Trump Organization likely took human action to re-establish access to the server when it was interrupted.

Again, the DNS traces will not by themselves reveal the nature of the special relationship that existed among the four entities. It could still be true that the machine was used by the four companies for some purpose unrelated to the Trump Organization (although the parties would have known they were using a "**trump-email.com**" name to access it).

Irrelevant and Incorrect Analysis

Our researchers reviewed an enormous amount of secondary analysis of the data in the media and web forums that is incorrect, irrelevant, or both. Some of these claims are enumerated below to address the inevitable, "but what about..." questions.

1. ***Incorrect: "The DNS traffic was a covert channel."***

It is possible to tunnel or conceal arbitrary data in the DNS protocol, and it is sometimes done to evade firewall restrictions or hide activity. To do this at any useful scale requires use of TXT

or other unusual DNS query times, or a high volume of queries, if information is to be hidden inside ordinary-looking DNS payloads. There are no signs of complex manipulation in the "mail1.trump-email.com" traffic, and there is not remotely enough volume for a steganographic technique (such as uppercase-encoding) to be viable.

2. ***Incorrect: "The Spectrum Health machine was a Tor exit node."***

It is unclear where this theory originated. Anyone can inspect the list of Tor exit nodes at any time. There is no reason to believe any of the IP addresses relevant to this case were ever part of Tor.

3. ***Irrelevant: "The Deep Discovery Inspector application creates DNS traffic."***

The Mandiant report released by lawyers for Alfa Bank describes a Trend Micro product named "*Deep Discovery Inspector*" (DDI). Mandiant found that DDI issued "*11 automated DNS requests within the first 14 seconds*" of receipt of an email containing a fictitious domain name in the body of the text. Even assuming this is true, it does not matter. As the Mandiant report indicates, the only examples of spam email containing "trump-email.com" to Alfa that have ever been produced are from dates prior to February 5, 2016—well before the period of interest. Notably, no DNS queries were seen from Alfa Bank in the DNS data-set from January 1, 2016, to May 3, 2016.

A second problem with the DDI hypothesis is that the Mandiant report found that DDI issued both A and AAAA queries. However, AAAA queries were never seen in the DNS logs collected during the period of interest.

4. ***Irrelevant: "The Alfa firewall would have blocked direct communication on mail ports between Alfa-Bank DNS servers and mail1.trump-email.com."***

Even if the wildest conspiracy theory were true, there is no reason for an Alfa Bank DNS server to attempt to connect to port 25 on "mail1.trump-email.com." This claim, from the "management sumary" (sic) of the Mandiant report, not substantiated in the report body, is meaningless.

5. ***Irrelevant: "The DNS records do not prove two-way communication."***

This claim has been made in public relations statements (i.e. by Cendyn) and even by "expert" observers. It is technically accurate that the DNS logs do not prove that communication took place. But it is a misleading statement. DNS queries do not carry the content of the communication, but neither do they happen for no reason. They happen when a server is attempting to communicate.

Lacking evidence for any spurious cause for the queries, such as a specifically misconfigured machine, the simplest and most reasonable assumption is that the DNS traffic was created by application-layer software attempting to open a TCP connection. And there is no reasonable assumption for why software would attempt to open a connection except that it wanted to exchange information (i.e. communicate).

6. ***Irrelevant: "trump-email.com was registered by Cendyn, not Trump."***

This is not contested, it simply re-confirms that Cendyn operated a server of some kind on behalf of the Trump Organization. It says nothing about what that server was used for, or by whom.

7. ***Irrelevant: "Cendyn used to send marketing email on behalf of Trump Organization."***

This is not contested. Examples have been produced that are years old. However, no email containing "trump-email.com" during the period of interest has ever been identified, despite significant efforts to locate such email. By the Mandiant report's description of its own content, if Alfa Bank had any emails, Mandiant should have been able to locate them.

8. ***Irrelevant: The entire Stroz Friedberg report.***

A document titled "*Summary of Cyber Incident Investigation*" was commissioned by Alfa Bank, written by "Stroz Friedberg, LLC," and submitted to the Senate by then-Department of Justice nominee Brian Benczkowski. The document's own introduction explains its irrelevancy: "*Alfa Bank engaged Stroz Friedberg on March 14, 2017*" to review "*suspicious entries in its DNS logs*" from February and March 2017. No matter what could be found in DNS and forensic logs at Alfa Bank from February 2017, it has nothing to do with the 2016 period of interest.

9. ***Incorrect: "The DNS look-ups of the Trump Organization Server was DDoS attack."***

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. The look-ups of the Trump Organization Server were miniscule in both total number and in number of sources.